MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

FABIANO DE MORAES DOMINGUES

PREVENÇÃO CONTRA FRAUDE EM CRIPTOGRAFIA VISUAL COM BASE NA AUTENTICAÇÃO DE MÚLTIPLAS IMAGENS EM TRANSPARÊNCIAS CIRCULARES

Rio de Janeiro
2013

INSTITUTO MILITAR DE ENGENHARIA

FABIANO DE MORAES DOMINGUES

PREVENÇÃO CONTRA FRAUDE EM CRIPTOGRAFIA VISUAL COM BASE NA AUTENTICAÇÃO DE MÚLTIPLAS IMAGENS EM TRANSPARÊNCIAS CIRCULARES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. José Antônio Moreira Xexéo - D.Sc.

Rio de Janeiro
2013

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80-Praia Vermelha
Rio de Janeiro-RJ CEP 22290-270

005.82 Domingues, Fabiano de Moraes
D671p Prevenção contra fraude em Criptografia Visual com base na autenticação de múltiplas imagens em transparências circulares / Fabiano de Moraes Domingues; orientado por José Antônio Moreira Xexéo. - Rio de Janeiro: Instituto Militar de Engenharia, 2013.

92 p.: il.

Dissertação (mestrado). – Instituto Militar de Engenharia – Rio de Janeiro, 2013.

1. Criptografia Visual. 2. Fraude. 3. Prevenção. I. Xexéo, José Antônio Moreira. II. Título. III. Instituto Militar de Engenharia.

CDD 005.82

INSTITUTO MILITAR DE ENGENHARIA

FABIANO DE MORAES DOMINGUES

PREVENÇÃO CONTRA FRAUDE EM CRIPTOGRAFIA VISUAL COM BASE NA AUTENTICAÇÃO DE MÚLTIPLAS IMAGENS EM TRANSPARÊNCIAS CIRCULARES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. José Antônio Moreira Xexéo - D.Sc.

Aprovada em 06 de fevereiro de 2013. pela seguinte Banca Examinadora:

Prof. José Antônio Moreira Xexéo - D.Sc. do IME - Presidente

Prof. Anderson Fernandes Pereira dos Santos - D.Sc. do IME

Prof. Luiz Manoel Silva de Figueiredo - Ph.D. da UFF

Prof. Eduardo Bezerra da Silva - D.Sc. do CEFET-RJ

Rio de Janeiro
2013

Dedico esta dissertação à minha família humana e canina.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram com o desenvolvimento desta dissertação de mestrado, em especial ao meu orientador Prof. D.Sc. José Antônio Moreira Xexéo, por ter confiado a mim sua amizade e dedicado a sua experiência ao nosso projeto de pesquisa. Desde a nossa primeira reunião, que ocorreu na aula inaugural do curso, respeitou as minhas limitações como pesquisador e optou por acreditar no meu potencial.

Também agradeço a todos os professores e funcionários da Seção de Engenharia de Computação (SE/8) do Instituto Militar de Engenharia.

Fabiano de Moraes Domingues

"Tudo o que a sua mão encontrar para fazer, faça-o com todo o seu coração."

JESUS

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABREVIATURAS

ABCPS	-	*Authentication Based Cheating Prevention scheme*
EVCS	-	*Extended Visual Cryptography Scheme*
NSA	-	*National Security Agency*
TS	-	*Threshold Scheme*
VCS	-	*Visual Cryptography Scheme*

RESUMO

Em Criptografia Visual, a partir de uma imagem secreta composta por pixels pretos e brancos, é possível gerar n transparências de forma que essa imagem se torne visível quando forem sobrepostas determinada quantidade $q \geq k$ dessas transparências e totalmente invisível caso $q < k$. Foi demonstrado que este esquema é vulnerável contra fraude quando $k = 2$ e $n > 2$.

Um esquema de prevenção contra a fraude baseado na autenticação de imagens fornece a capacidade de verificação da integridade das transparências antes que a imagem secreta seja decodificada. Os principais esquemas deste tipo, chamados de HCT e HT sofreram ataques às suas vulnerabilidades identificadas.

O principal objetivo deste trabalho é apresentar a construção de um novo esquema de prevenção contra fraude que forneça a capacidade de detecção da fraude com suporte aos aspectos de segurança relacionados com a proteção aos ataques realizados contra os esquemas anteriores HCT e HT.

A Criptografia Visual de múltiplas imagens forneceu a estrutura básica para a construção dos mecanismos de detecção da fraude e de proteção contra os ataques conhecidos. O suporte aos aspectos de segurança contra as vulnerabilidades dos esquemas HCT e HT pode ser resumido em: possibilitar a verificação de cada transparência em toda sua extensão; limitar a quantidade de pixels pretos das imagens de verificação; permutar as posições das imagens que serão autenticadas durante o processo de verificação da integridade das transparências; e aumentar a expansão dos pixels para incorporar informações adicionais, com definição aleatória na autenticação ou construção dos blocos.

ABSTRACT

In Visual Cryptography, from a secret image composed of black and white pixels, it is possible to generate n transparencies so that this image becomes visible when superimposed quantity $q \geq k$ these transparencies and totally invisible case $q < k$. It has been shown that this scheme is vulnerable against cheat when $k = 2$ and $n > 2$.

A scheme of cheat prevention based authentication images provides the ability to verify the integrity of transparencies before the secret image is decoded. The main schemes of this type, called HCT and HT suffered attacks on their vulnerabilities identified.

The main objective of this paper is to present the construction of a new cheat prevention scheme that provides the ability to detect cheat with support for security aspects related to protection to attacks against the previous schemes HCT and HT.

The Visual Cryptography of multiple images provided the basic framework for the construction of mechanisms to detect cheat and protection against known attacks. The support for aspects of security against vulnerabilities schemes HCT and HT can be summarized in: permit verification of each transparency throughout its length; limiting the amount of black pixels of the verification images; swapping the positions of the images to be authenticated during the process of verifying the integrity of the transparencies; and increase the expansion of pixels to incorporate additional information, with random setting in authentication or building blocks.

1 INTRODUÇÃO

A confidencialidade de qualquer informação secreta pode ser obtida através da Criptografia. Sistemas criptográficos convencionais foram definidos por SHANNON (1949) como uma família de transformações unicamente inversíveis de um conjunto de possíveis mensagens em um conjunto de criptogramas. Cada transformação corresponde a um processo de codificação com uma chave específica. As transformações são unicamente inversíveis para que a decodificação seja possível quando a chave for conhecida.

Com o objetivo de complementar os trabalhos sobre Criptografia, que à sua época descreviam diversos padrões de cifras e as formas de decifrá-las, SHANNON (1949) definiu a estrutura matemática e as propriedades relacionadas com os sistemas criptográficos, através de um artigo considerado por DIFFIE e HELLMAN (1979) como um trabalho fundamental para o estudo da Criptografia, por conter a base da teoria da informação para a criptoanálise clássica, além de caracterizar os sistemas criptográficos perfeitos e descrever a construção de alguns padrões de cifras.

A teoria definida por SHANNON (1949) presume que o criptoanalista possui poder computacional ilimitado. Por este motivo, HELLMAN (1977) havia considerado que a principal utilidade desta teoria seria a obtenção de percepções qualitativas na concepção de sistemas criptográficos. No entanto, ela não poderia ser aplicada diretamente no desenvolvimento prático de novos sistemas.

Em oposição às afirmações de HELLMAN (1977), o sistema criptográfico considerado pela NSA[1] através de KLEIN (2003) como um dos mais importantes da história da Criptografia é um sistema perfeito, de acordo com a definição de SHANNON (1949). Este sistema foi desenvolvido durante a 1^a guerra mundial e registrado por VERNAM (1919) sob a patente U.S. 1.310.719. As especificações do sistema foram publicadas por VERNAM (1926).

De acordo com SHANNON (1949), cada chave utilizada na proteção das informações deve ser transmitida em canais protegidos contra interceptação da origem até o destino. A proteção das chaves utilizadas na cifragem da informação deve ser obtida através de um método especial. Um sistema de armazenamento deve manter as chaves em locais prote-

[1]National Security Agency

gidos na memória, pois um incidente pode tornar a informação inacessível. É importante manter outras cópias com pessoas confiáveis ou em locais seguros. Diante da necessidade de armazenar de forma segura as chaves criptográficas, BLAKLEY (1979) apresentou o seguinte dilema: "se um determinado sistema de armazenamento gera muitas cópias, torna-se difícil evitar a perda. Por outro lado, se o sistema cria um número reduzido de cópias, todas poderão ser destruídas". As cópias das chaves ou as partes da informação que reconstroem a chave devem ser protegidas contra diversos tipos de incidentes.

Uma forma útil de armazenar chaves criptográficas foi criada por SHAMIR (1979). Ele considerou que este é um problema relacionado com o compartilhamento de um segredo, que pode ser realizado através da divisão de um dado secreto D em n partes $D_1, ..., D_n$, de forma que o conhecimento de determinada quantidade $q \geq k$ dessas partes tornaria D facilmente calculável, e completamente indeterminado caso $q < k$.

Este esquema foi definido por SHAMIR (1979) como um $(k, n)TS$[2] e é ideal em aplicações formadas por um grupo de indivíduos mutuamente suspeitos, com interesses conflitantes, mas que devem cooperar entre si. Em outras palavras, um $(k, n)TS$ é útil quando alguma informação deve ser replicada ou dividida por n participantes ou locais, e protegida contra $k - 1$ violações de segurança, devido a fragilidade dos dados ou desconfiança entre esses participantes.

Sobre a desconfiança entre os participantes, TOMPA e WOLL (1989) adicionaram a seguinte propriedade ao $(k, n)TS$ de SHAMIR (1979): existe a possibilidade de que quaisquer $k - 1$ participantes $P_1, ..., P_{k-1}$ possam construir novas partes $D'_1, ..., D'_{k-1}$ com o objetivo de enganar o k-ésimo participante P_k. Determinar que P_k foi enganado significa concluir que o dado secreto D', reconstruído pela junção entre as partes falsas $D'_1, ..., D'_{k-1}$ e a parte original D_k, foi considerado legal, apesar de ser incorreto, pois $D \neq D'$. Com a adição desta propriedade, TOMPA e WOLL (1989) afirmaram que o esquema de SHAMIR (1979) é vulnerável à fraude definida por eles.

Diante deste cenário, uma abordagem visual da Criptografia sobre o $(k, n)TS$ foi desenvolvida por NAOR e SHAMIR (1995) e definida por eles como $(k, n)VCS$[3]. A partir de uma imagem secreta, composta por pixels pretos e brancos, é possível gerar n transparências, de forma que essa imagem se torne visível quando determinada quantidade $q \geq k$ dessas transparências for sobreposta e completamente invisível caso $q < k$. Uma

[2]Threshold Scheme

[3]Visual Cryptography Scheme

abordagem interessante que descreve o relacionamento entre o $(k, n)TS$ e o $(k, n)VCS$ foi realizada por STINSON (1999).

Um $(2, 2)VCS$ é a estrutura mais simples em Criptografia Visual e pode ser utilizada como um sistema criptográfico convencional na codificação de materiais impressos como imagens, documentos e até textos escritos à mão. Um sistema criptográfico baseado no $(2, 2)VCS$ é composto por uma página que contém a imagem impressa do criptograma e por uma transparência que possui a imagem impressa da chave. As imagens impressas na página e na transparência não revelam qualquer informação sobre a imagem original, que pode ser reconstruída somente através da sobreposição entre elas.

Devido a sua simplicidade, um $(k, n)VCS$ pode ser utilizado por qualquer pessoa sem conhecimento prévio sobre Criptografia e sem a utilização de qualquer tipo de processamento computacional na reconstrução da imagem secreta, pois esse processo é realizado diretamente pelo sistema visual humano.

De acordo com NAOR e SHAMIR (1996), um $(k, n)VCS$ fornece a segurança incondicional, de acordo com as definições de SHANNON (1949). Através de uma comparação realizada com o sistema de VERNAM (1926), NAOR e SHAMIR (1996) constataram que a única diferença é a operação booleana utilizada. Um $(k, n)VCS$ é baseado na operação OU, enquanto que a cifra de VERNAM (1926) é baseada na operação XOR.

No entanto, é possível observar que somente o $(2, 2)VCS$ fornece segurança incondicional, definida por SHANNON (1949), pois um $(k, n)VCS$ com outras configurações de k e n, mais especificamente quando $k = 2$ e $n > 2$ é vulnerável à fraude definida por TOMPA e WOLL (1989) e aplicada no contexto da Criptografia Visual por HORNG, CHEN e TSAI (2006). Eles demonstraram que $n-1$ participantes desonestos são capazes de fraudar a imagem secreta em um $(2, n > 2)VCS$ quando trabalham em conjunto com o objetivo de enganar o participante honesto.

1.1 MOTIVAÇÃO

A fraude pode ser evitada, se o n-ésimo participante for capaz de suspeitar que as transparências dos outros $n - 1$ participantes não são originais ou que a imagem reconstruída após uma sobreposição não é verdadeira. De acordo com HORNG, CHEN e TSAI (2006), a solução natural para o problema da fraude deve ser obtida através do conceito de autenticação em Criptografia Visual, introduzido por NAOR e PINKAS (1997). Este tipo

de esquema é conhecido como um $ABCPS$[4] e fornece aos participantes a capacidade de verificar a integridade das outras transparências antes que o processo de reconstrução da imagem secreta seja realizado.

Algumas vantagens e desvantagens em relação a um $ABCPS$ podem ser verificadas. Duas vantagens foram apresentadas por CIMATO e YANG (2011). A primeira está relacionada com o fato de que a verificação de integridade das transparências é opcional e pode ser realizada apenas quando algum participante suspeita de fraude. A segunda vantagem está relacionada com a geração das transparências de verificação, que deve ser realizada após a geração das transparências originais. Por este motivo, qualquer estrutura de acesso pode ser transformada em um esquema de prevenção contra fraude. Duas desvantagens foram apresentadas por LIU, WU e LIN (2011) e CIMATO e YANG (2011). De acordo com LIU, WU e LIN (2011), um $ABCPS$ requer transparências extras de verificação, recurso que inevitavelmente aumenta a carga sobre os participantes. CIMATO e YANG (2011) afirmaram que não é possível realizar uma prova formal de segurança para este tipo de esquema.

Outras técnicas foram utilizadas em alguns esquemas de prevenção contra fraude. Os esquemas de HU e TZENG (2007) e PRISCO e SANTIS (2006) aumentam a expansão do pixel para incorporar informações adicionais de autenticação. Um dos esquemas de HORNG, CHEN e TSAI (2006) gera um número maior do que n transparências para reduzir o conhecimento que os participantes desonestos possuem sobre a distribuição dos pixels na transparência da vítima. Finalmente, o esquema de TSAI, CHEN e HORNG (2007) utiliza algoritmo genético para codificar imagens secretas homogêneas.

Os dois principais esquemas de prevenção contra fraude foram desenvolvidos por HORNG, CHEN e TSAI (2006) e HU e TZENG (2007). Esses esquemas são do tipo $ABCPS$ e serão nomeados neste trabalho como HCT e HT, respectivamente, como referências às iniciais dos seus criadores. Sobre o esquema de prevenção HCT, dois ataques foram realizados por HU e TZENG (2007) e LIU, WU e LIN (2011). Sobre o esquema de prevenção HT, um ataque foi realizado por LIU, WU e LIN (2011). Devido aos ataques realizados, um $(2, n)VCS$ baseado em um dos esquemas de prevenção HCT ou HT permanece vulnerável à fraude.

[4]Authentication Based Cheating Prevention scheme

1.2 OBJETIVOS

O projeto de um esquema de prevenção deve fornecer a capacidade de detecção da fraude demonstrada por HORNG, CHEN e TSAI (2006) em um $(2, n)VCS$ com suporte adicional aos aspectos de segurança relacionados com a proteção contra os ataques realizados sobre os esquemas HCT e HT. O principal objetivo deste trabalho é a construção de um esquema de prevenção $ABCPS$ que forneça a qualquer participante a capacidade de detectar a fraude, caso desconfie que os outros participantes não sejam honestos, por suspeitar que as suas transparências não sejam originais e que a imagem reconstruída após uma sobreposição não seria verdadeira.

A estrutura que fornece os mecanismos de detecção da fraude e o suporte aos aspectos de segurança contra as vulnerabilidades conhecidas consiste em: possibilitar a verificação de cada transparência em toda sua extensão através da construção de uma versão adaptada do esquema de múltiplas imagens desenvolvido por SHYU et al. (2007); limitar a quantidade de pixels pretos das imagens de verificação através da utilização de um módulo de validação; permutar as posições das imagens que serão autenticadas durante o processo de verificação da integridade das transparências; e aumentar a expansão dos pixels para incorporar informações adicionais, com definição aleatória na autenticação ou construção dos blocos de cada transparência.

O segundo objetivo deste trabalho é fornecer uma análise sobre os ataques realizados contra o HCT e o HT, com base na demonstração através de experimentos das vulnerabilidades exploradas por eles e na apresentação de sugestões sobre possíveis correções aos esquemas. Esta análise forma a base para a construção de um novo esquema de prevenção contra fraude em Criptografia Visual, objetivo principal deste trabalho.

1.3 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em sete capítulos. No Capítulo 1 foi apresentada a motivação para a realização do trabalho, assim como os objetivos a serem alcançados. No Capítulo 2 serão apresentadas algumas definições básicas que relacionam os sistemas criptográficos definidos por SHANNON (1949) como perfeitos ao $(2, 2)VCS$. Também no Capítulo 2, a estrutura do $(2, 2)VCS$ será apresentada através de dois experimentos que demonstram as sobreposições das transparências construídas com base nesse esquema. Em seguida, será demonstrado o esquema de SHYU et al. (2007), que permite a codificação

de múltiplas imagens, com o objetivo de fornecer a base conceitual para a definição do novo esquema de prevenção contra fraude desenvolvido neste trabalho.

No Capítulo 3 será apresentada a estrutura do $(2, n > 2)VCS$ através dos seus conceitos básicos e de um experimento que demonstra a construção e a sobreposição das transparências. Também no Capítulo 3 será vinculado ao $(2, n > 2)VCS$ a vulnerabilidade relacionada com a fraude definida por HORNG, CHEN e TSAI (2006), através de um experimento que demonstra o sucesso dos participantes desonestos.

No Capítulo 4, os dois principais esquemas de prevenção contra a fraude serão apresentados, através de suas definições básicas e de dois experimentos que demonstram o funcionamento do HCT e do HT em um $(2, 3)VCS$. Também no Capítulo 4 serão descritos os três ataques relacionados com esses esquemas através da apresentação dos conceitos principais e de experimentos que comprovam o sucesso do primeiro ataque contra o HCT e do único ataque contra o HT. Será demonstrado, através de alguns experimentos que o sucesso do segundo ataque contra o HCT pode ser atingido mediante o cumprimento de alguns pré-requisitos. Uma análise sobre cada um dos três ataques, assim como as correções necessárias para tornar os esquemas seguros contra eles conclui o Capítulo 4.

O Capítulo 5 trata do esquema de prevenção contra fraude desenvolvido neste trabalho, através de definições especificamente relacionadas com a construção das transparências originais e circulares de verificação, que devem ser entregues aos participantes, assim como de um módulo capaz de validar as imagens que devem ser autenticadas durante o processo de verificação da integridade das transparências dos outros participantes. Também no Capítulo 5, serão apresentados os experimentos necessários para a demonstração do funcionamento da nova prevenção em um $(2, 3)VCS$.

No Capítulo 6, os aspectos de segurança relacionados com o novo esquema de prevenção serão discutidos. Uma adaptação do método de realização da fraude será apresentada, assim como sua detecção, através de experimentos realizados que demonstram essas ações. Também no Capítulo 6, será demonstrada e execução de um novo ataque contra o esquema de prevenção construído neste trabalho e apresentado no Capítulo 5, baseado na combinação e adaptação das técnicas utilizadas contra os esquemas HCT e HT, com o objetivo de demonstrar sua resistência contra os ataques conhecidos.

O trabalho será concluído no Capítulo 7, através de uma análise geral dos objetivos alcançados e dos trabalhos futuros que podem dar continuidade a esta pesquisa.

2 SISTEMAS CRIPTOGRÁFICOS

O objetivo deste Capítulo é apresentar uma introdução à Criptografia Visual, além de relacionar seus principais esquemas com os sistemas criptográficos perfeitos, que fornecem segurança incondicional. Este Capítulo está organizado da seguinte forma. Na Seção 2.1, a estrutura básica de um sistema criptográfico clássico será apresentada, de acordo com a definição de SHANNON (1949). Na Seção 2.2, serão apresentados os conceitos sobre segurança incondicional e computacional, que revelam dois pontos de vista diferentes: a segurança incondicional é fornecida por sistemas perfeitos, segundo a definição de SHANNON (1949) e a segurança computacional pode ser encontrada no sistema de chave pública desenvolvido por DIFFIE e HELLMAN (1976), de acordo com a definição de HELLMAN (1977). Na Seção 2.3, os conceitos básicos sobre sistemas perfeitos serão discutidos. Na Seção 2.4, será apresentada a Criptografia Visual, introduzida por NAOR e SHAMIR (1995) através da estrutura $(2, 2)VCS$, que pode ser utilizada como um sistema criptográfico clássico e fornece segurança incondicional, de acordo com NAOR e SHAMIR (1996). Em seguida, dois experimentos que demonstram a utilização do $(2, 2)VCS$ serão apresentados. Na Seção 2.5, será apresentado o esquema de SHYU et al. (2007), que está inserido no contexto da Criptografia Visual de múltiplas imagens, através de um experimento que demonstra a codificação de três imagens secretas em duas transparências circulares. Finalmente, o Capítulo será concluído na Seção 2.6 através de uma breve análise sobre a segurança dos esquemas de Criptografia Visual apresentados.

2.1 DEFINIÇÕES BÁSICAS

Sistemas criptográficos convencionais foram definidos por SHANNON (1949) como uma família de transformações unicamente inversíveis de um conjunto de possíveis mensagens em um conjunto de criptogramas. Cada transformação corresponde a um processo de codificação com uma chave específica, que deve ser transmitida em canais protegidos contra interceptação da origem até o destino. As transformações são unicamente inversíveis para que a decodificação seja possível quando a chave for conhecida. Duas abordagens detalhadas sobre sistemas criptográficos foram realizadas por MENEZES, VAN OORSCHOT e VANSTONE (1996) e STALLINGS (2005).

O fluxo da transmissão de uma mensagem em um sistema criptografico clássico é apresentado na FIG. 2.1. A transmissão de mensagens criptografadas depende de duas fontes de informação: uma fonte de chaves e uma fonte de mensagens. A fonte de chaves é responsável pela produção de uma chave específica K entre todas que são possíveis no sistema. A chave é transmitida por algum canal, supostamente seguro contra interceptação, até o ponto de destino. A fonte de mensagens é responsável pela produção de uma mensagem específica M para ser criptografada. O criptograma resultante C é enviado por um meio possivelmente inseguro contra interceptação, até o ponto de destino. O ponto de destino é responsável por utilizar a chave combinada K para decifrar o criptograma C e recuperar a mensagem M.

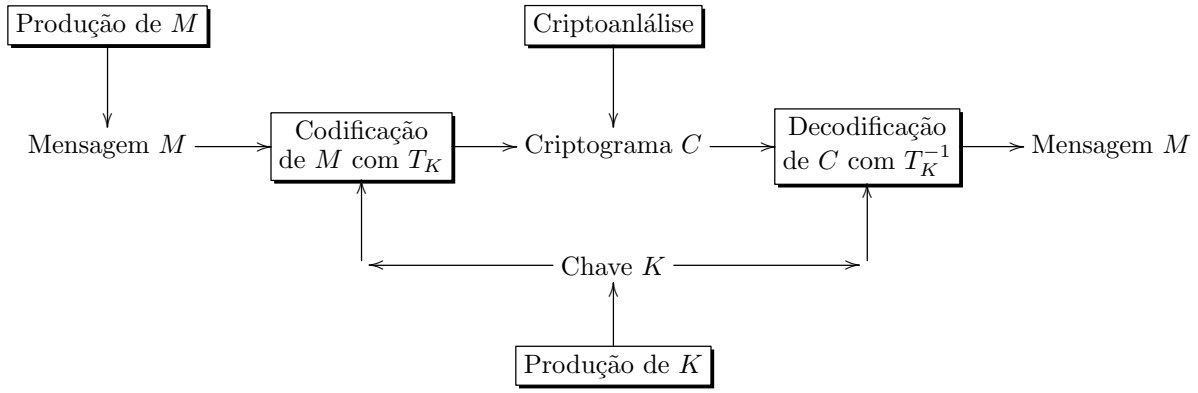


FIG. 2.1: Sistema criptográfico clássico. Adaptação: (SHANNON, 1949).

A codificação da mensagem M é realizada a partir de $C = f(M, K)$, de forma que C seja obtido em função de M e K. Sobre esta função de duas variáveis, SHANNON (1949) definiu outra abordagem, através de um parâmetro único, representado por uma família de transformações, definida como $C = T_K M$, onde a transformação T_K aplicada na mensagem M produz o criptograma C, e K representa a chave específica utilizada.

É possível assumir que o conjunto de chaves seja finito e que cada chave K possua uma probabilidade P_K associada. Desta forma, a fonte de chaves é representada por um processo estatístico ou um dispositivo que escolhe somente uma, a partir de um conjunto de transformações com suas respectivas probabilidades. Um conjunto finito de possíveis mensagens está associado com suas respectivas probabilidades *a priori*.

Na extremidade receptora, é possível recuperar M, através do conhecimento de C e K. Portanto, as transformações T_K da família devem ter inversas únicas T_K^{-1}, de forma que $T_K T_K^{-1} = I$, a transformação identidade. Então, $M = T_K^{-1} C$.

2.2 SEGURANÇA INCONDICIONAL E COMPUTACIONAL

De acordo com HELLMAN (1977), a abordagem utilizada por DIFFIE e HELLMAN (1976) evidencia uma relação com a teoria da complexidade computacional. Essa teoria presume que o criptoanalista possui poder computacional finito, embora sua capacidade seja enorme. Na opinião de HELLMAN (1977), a teoria finita computacional suportaria diretamente a Criptografia prática e a teoria clássica de SHANNON (1949) seria útil principalmente em fornecer informações relevantes sobre os princípios dos projetos de sistemas criptográficos.

Nos sistemas criptográficos definidos por SHANNON (1949) como perfeitos, o poder do inimigo não é maior após a interceptação de qualquer quantidade de material do que antes, pois a quantidade de informação disponível é realmente insuficiente para determinar as transformações de cifragem e decifragem, não importa quanto poder computacional o inimigo tenha disponível. DIFFIE e HELLMAN (1976) classificaram esses sistemas como incondicionalmente seguros.

Entre os sistemas que produzem criptogramas com solução única, SHANNON (1949) afirmou que há grandes variações na quantidade de trabalho necessária para realizar esta solução e no valor do material que deve ser interceptado para encontrar a solução original. Mesmo que o material interceptado contenha informações suficientes para permitir a formação de uma solução única, não é possível garantir que um inimigo com recursos computacionais limitados será bem sucedido. DIFFIE e HELLMAN (1979) definiram que um sistema criptográfico, cuja segurança é condicionada ao custo computacional para a criptoanálise, mas que não resistiria à criptoanálise com poder de computação ilimitado, é classificado como computacionalmente seguro.

Embora a incapacidade da criptoanálise possa ser comprovada diante de um sistema criptográfico perfeito ou incondicionalmente seguro, DIFFIE e HELLMAN (1979) admitiram que a teoria da complexidade computacional é insuficiente para comprovar a inviabilidade computacional da solução de qualquer problema da criptoanálise, e que a Criptografia deve confiar em um processo de certificação de segurança menos formal ao submeter um sistema criptográfico às condições favoráveis para a criptoanálise.

O sistema de chave pública foi desenvolvido por DIFFIE e HELLMAN (1976), e independentemente, por MERKLE (1978). Este sistema foi registrado pelos três pesquisadores em 1980 sob a patente U.S. 4.200.770 e pode ser classificado como um sistema cuja segu-

rança é baseada na teoria da complexidade computacional. Sua principal implementação é a cifra desenvolvida por RIVEST, SHAMIR e ADLEMAN (1978), cuja segurança é baseada na incapacidade tecnológica atual em solucionar problemas matemáticos computacionalmente difíceis, e na limitação do conhecimento teórico das leis matemáticas, principalmente no que se refere à descoberta de novas técnicas de fatoração.

2.3 SISTEMAS PERFEITOS

Conforme foi apresentado na Seção 2.1, cada chave K é uma transformação T_K que possui uma probabilidade *a priori* associada, que significa a probabilidade relacionada à sua escolha. Da mesma forma, cada mensagem possui uma probabilidade *a priori* associada. A relação entre esses dois conjuntos de probabilidades representa o conhecimento *a priori* que o criptoanalista possui.

Caso o criptograma C seja interceptado pelo criptoanalista, então ele poderá calcular as probabilidades *a posteriori* das mensagens e chaves possíveis que poderiam ter produzido C. O conjunto de probabilidades *a posteriori* representa o conhecimento que o criptoanalista possui sobre as chaves e as mensagens após a interceptação do criptograma.

A segurança incondicional foi definida por SHANNON (1949) como um requisito verificado nos sistemas criptográficos perfeitos, que possuem as probabilidades *a posteriori* calculadas após o criptoanalista realizar a interceptação de seus criptogramas iguais às probabilidades *a priori* calculadas antes da interceptação. Para que a segurança incondicional seja obtida, é necessário que, caso o número de mensagens possíveis seja finito, que o número de chaves possíveis seja igual.

A definição formal sobre sistemas perfeitos apresentada por SHANNON (1949) é descrita a seguir. Seja o conjunto finito de mensagens possíveis $M_1, ..., M_n$, com probabilidades *a priori* definidas por $P(M_1), ..., P(M_n)$ e possíveis criptogramas $C_1, ..., C_n$ gerados por $C = T_K M$. Se um criptoanalista intercepta um criptograma específico C, então ele pode calcular as probabilidades *a posteriori* de várias mensagens. Portanto, para que um sistema seja incondicionalmente seguro é necessário que, para todo C, as probabilidades *a posteriori* sejam iguais às probabilidades *a priori*, independentemente de seus valores. Neste caso, a interceptação da mensagem não fornece ao criptoanalista qualquer informação. Se esta condição não for satisfeita, a escolha de determinadas chaves e mensagens pode mudar as probabilidades que o criptoanalista possui, e consequentemente influenciar as suas ações.

2.4 INTRODUÇÃO À CRIPTOGRAFIA VISUAL

O esquema de Criptografia Visual construído por NAOR e SHAMIR (1995) presume que uma imagem secreta deve ser composta por uma coleção de pixels pretos e brancos. Um pixel da imagem secreta é representado em cada transparência por uma coleção de m subpixels pretos e brancos, chamada de bloco B. O sistema visual humano interpreta as cores dos blocos como tons de cinza, definidos pela contribuição média dos subpixels pretos e brancos. A estrutura básica deste esquema é apresentada na FIG. 2.2.

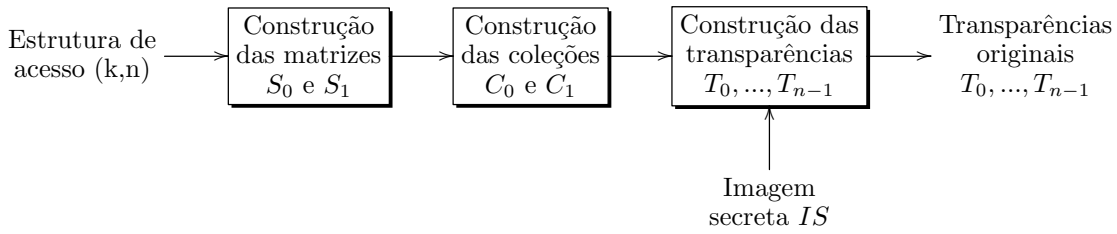


FIG. 2.2: Fluxo para a construção de $T_0, ..., T_{n-1}$. Adaptação: (CIMATO e YANG, 2011).

A partir de uma estrutura de acesso definida pelos parâmetros k e n, é possível construir duas matrizes binárias de dimensões $n \times m$, denominadas S_0 e S_1, com elementos s_{ij}, onde $s_{ij} = 1$ se o j-ésimo subpixel da i-ésima transparência for preto. O parâmetro m indica o número de subpixels em um bloco, e representa a perda de resolução da imagem secreta em comparação com a imagem reconstruída pela sobreposição das transparências.

O resultado da combinação dos blocos correspondentes a um determinado pixel da imagem secreta, quando as transparências $T_0, ..., T_{n-1}$ são sobrepostas é equivalente ao resultado da operação booleana OU das linhas $i_0, ..., i_{n-1}$ de S_0 ou S_1. O tom de cinza desta combinação é proporcional ao peso de *Hamming* $H(V)$ do vetor V de tamanho m, resultante da operação booleana OU. Este tom de cinza é interpretado pelo sistema visual humano como preto se $H(V) \geq d$ e como branco se $H(V) < d - \alpha.m$, para determinado *threshold* $1 \leq d \leq m$ e contraste relativo $\alpha > 0$.

O parâmetro α indica o contraste relativo, que representa a perda de contraste em relação à imagem secreta. Ele é definido pela razão entre o número máximo de subpixels pretos em um bloco resultante correspondente a um pixel branco, e o número mínimo de subpixels pretos em um bloco resultante correspondente a um pixel preto da imagem secreta. BLUNDO, DE SANTIS e STINSON (1999) e BLUNDO et al. (2003) realizaram algumas pesquisas, com o objetivo de definir construções de esquemas em Criptografia Visual baseadas na otimização do contraste relativo das imagens reconstruídas.

Após a construção das matrizes S_0 e S_1, o esquema define duas coleções de matrizes binárias de dimensões $n \times m$, denominadas C_0 e C_1. As coleções C_0 e C_1 são formadas por todas as matrizes obtidas pelas permutações das colunas de S_0 e S_1.

A etapa seguinte é a construção das transparências $T_0, ..., T_{n-1}$. Sejam $B_p^{T_0}, ..., B_p^{T_{n-1}}$ os blocos das transparências $T_0, ..., T_{n-1}$, que correspondem ao p-ésimo pixel da imagem secreta IS. Para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel for branco, o esquema escolhe aleatoriamente uma das matrizes em C_0, e para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel for preto, o esquema escolhe aleatoriamente uma das matrizes em C_1. Nos dois casos, a matriz escolhida para codificar o p-ésimo pixel da imagem secreta IS define em cada linha i, as cores dos m subpixels do bloco $B_p^{T_i}$.

Dois experimentos baseados no $(2,2)VCS$ serão apresentadas nesta Seção. Os participantes convidados são os famosos personagens do mundo da Criptografia: Alice e Bob. Carol será convidada a partir do Capítulo 3, quando for necessário mais um participante nos experimentos. Alice e Bob devem receber as transparências T_A e T_B, respectivamente. No primeiro experimento, os parâmetros utilizados serão $m = 2$ e $\alpha = \frac{1}{2}$. As matrizes S_0 e S_1 podem ser construídas da seguinte forma:

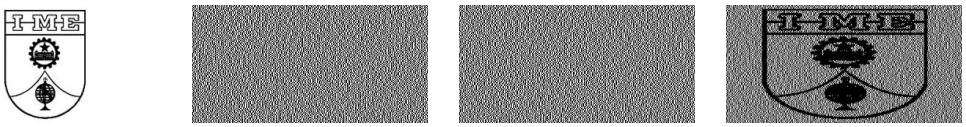
$$S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}; S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Conforme foi explicado anteriormente, as coleções C_0 e C_1 são formadas pelas matrizes obtidas através de todas as permutações possíveis das colunas de S_0 e S_1. As construções possíveis dos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que correspondem ao p-ésimo pixel da imagem secreta IS seguem a TAB. 2.1.

TAB. 2.1: Construções de $B_p^{T_A}$ e $B_p^{T_B}$ em um $(2,2)VCS$ com $m = 2$.

Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_A} + B_p^{T_B}$
1				
2				

No primeiro caso da TAB. 2.1, o p-ésimo pixel da imagem secreta IS é branco. Ele pode ser codificado de duas formas diferentes, com probabilidade $\frac{1}{2}$ de ocorrência, expandido nos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que se equivalem no bloco resultante da sobreposição $B_p^{T_A} + B_p^{T_B}$. No segundo caso da TAB. 2.1, o p-ésimo pixel da imagem secreta IS é preto. Ele também pode ser codificado de duas formas diferentes, com probabilidade $\frac{1}{2}$ de ocorrência, expandido nos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que se complementam no bloco resultante da sobreposição $B_p^{T_A} + B_p^{T_B}$. O resultado do experimento é apresentado na FIG. 2.3.



(a) IS (b) T_A (c) T_B (d) $T_A + T_B$

FIG. 2.3: Demonstração de $T_A + T_B = IS$ em um $(2,2)VCS$ com $m = 2$.

Na FIG. 2.3, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. As duas transparências T_A e T_B, que podem ser visualizadas nos itens (b) e (c), respectivamente, foram construídas a partir da IS. Cada T_i possui 150×300 pixels. A sobreposição $T_A + T_B$, que pode ser visualizada no item (d), define a reconstrução da IS.

No segundo experimento baseado no $(2,2)VCS$ que será apresentada nesta Seção, os parâmetros utilizados serão $m = 4$ e $\alpha = \frac{1}{2}$. As duas matrizes S_0 e S_1 podem ser construídas da seguinte forma:

$$S_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}; S_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

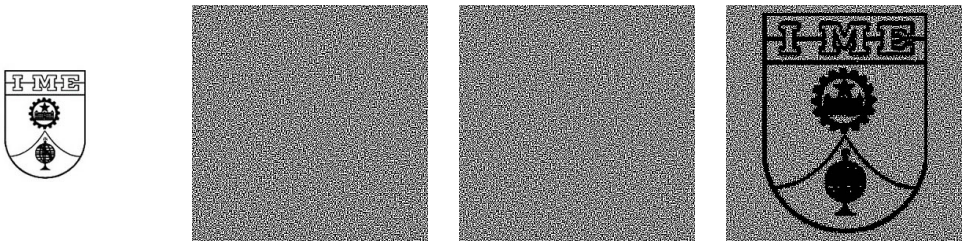
O procedimento utilizado no experimento anterior, cujo resultado foi demonstrado na FIG. 2.3, será executado novamente, ou seja, as coleções C_0 e C_1 serão formadas pelas matrizes obtidas através de todas as permutações possíveis das colunas de S_0 e S_1. As construções possíveis dos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que correspondem ao p-ésimo pixel da imagem secreta IS seguem a TAB. 2.2.

No primeiro caso da TAB. 2.2, o p-ésimo pixel da imagem secreta IS é branco. Ele pode ser codificado de seis formas diferentes, com probabilidade $\frac{1}{6}$ de ocorrência, expandido nos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que se equivalem no bloco resultante da sobreposição $B_p^{T_A} + B_p^{T_B}$. No

TAB. 2.2: Construções de $B_p^{T_A}$ e $B_p^{T_B}$ em um $(2,2)VCS$ com $m = 4$.

Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_A} + B_p^{T_B}$	Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_A} + B_p^{T_B}$
1	□	▚	▚	■	2	■	▚	▚	■
	□	▞	▞	■		■	▞	▞	■
	□	▖▗	▖▗	▖▗		■	▖▗	▖▗	■
	□	▘▝	▘▝	▘▝		■	▘▝	▘▝	■
	□	▀	▀	▀		■	▀	▖▗	■
	□	▄	▄	▄		■	▄	▘▝	■

segundo caso da TAB. 2.2, o p-ésimo pixel da imagem secreta IS é preto. Ele também pode ser codificado de seis formas diferentes, com probabilidade $\frac{1}{6}$ de ocorrência, expandido nos blocos $B_p^{T_A}$ e $B_p^{T_B}$, que se complementam no bloco resultante da sobreposição $B_p^{T_A} + B_p^{T_B}$. O resultado do experimento é apresentado na FIG. 2.4.



(a) IS (b) T_A (c) T_B (d) $T_A + T_B$

FIG. 2.4: Demonstração de $T_A + T_B = IS$ em um $(2,2)VCS$ com $m = 4$.

Na FIG. 2.4, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. As duas transparências T_A e T_B, que podem ser visualizadas nos itens (b) e (c), respectivamente, foram construídas a partir da IS. Cada T_i possui 300×300 pixels. A sobreposição $T_A + T_B$, que pode ser visualizada no item (d), define a reconstrução da IS.

2.5 CODIFICAÇÃO DE MÚLTIPLAS IMAGENS SECRETAS

Conforme foi apresentado na Seção 2.4, o esquema de Criptografia Visual construído por NAOR e SHAMIR (1995) codifica somente uma imagem secreta. Há uma disciplina da Criptografia Visual que trata da codificação de múltiplas imagens secretas.

Esta disciplina foi introduzida por WU e CHEN (1998). O esquema desenvolvido por eles é capaz de codificar duas imagens secretas IS_0 e IS_1 em duas transparências T_0 e T_1, de forma que a primeira imagem secreta IS_0 pode ser reconstruída através de uma sobreposição convencional $T_0 + T_1$. A reconstrução da segunda imagem secreta IS_1 deve ser obtida através da sobreposição $T_0 + T_1$ com rotação de 90^o, 180^o ou 270^o em T_0 ou T_1.

A restrição aos ângulos foi superada pelo esquema de HSU, CHEN e LIN (2004), que é capaz de codificar duas imagens secretas IS_0 e IS_1 em duas transparências circulares T_0 e T_1, com rotação em ângulos arbitrários. Esse esquema presume que as duas transparências circulares devem ser construídas e posicionadas como dois cilindros, de forma que o alinhamento correto entre elas permite a reconstrução da primeira imagem secreta IS_0 e a rotação de uma das transparências em determinado ângulo deve reconstruir a segunda imagem secreta IS_1.

Embora o esquema de HSU, CHEN e LIN (2004) seja de implementação mais fácil que o apresentado por WU e CHEN (1998), ainda possui a restrição relacionada com a codificação de duas imagens secretas IS_0 e IS_1 somente. Essa limitação foi superada pelo esquema construído por SHYU et al. (2007).

O esquema criado por SHYU et al. (2007) codifica n imagens secretas $IS_0, ..., IS_{n-1}$ em duas tranparências circulares T_0 e T_1 e requer a construção de T_0 e T_1 como cilindros, de forma que cada T_i seja obtido através da junção entre as suas extremidades laterais. A sobreposição entre T_0 e T_1 é realizada através de um encaixe de T_0 em T_1. A reconstrução de $IS_0, ..., IS_{n-1}$ pode ser obtida através de n posicionamentos diferentes de T_0 em relação à T_1. O posicionamento de cada sobreposição deve ser obtido através da rotação em $\theta = \frac{360^o}{n}$ graus de T_0, com relação ao posicionamento anterior.

Cada IS_j é reconstruída através da sobreposição entre T_0 e T_1, denotada por $T_0^{\theta \times j} \otimes T_1$, que representa o posicionamento de T_0 encaixado em T_1 com rotação de T_0 em n ângulos diferentes, definidos por $\theta \times j$. Por exemplo, é possível codificar 3 imagens secretas IS_0, IS_1 e IS_2 nas transparências circulares T_0 e T_1, de forma que a reconstrução de cada IS_j deve ser obtida da seguinte forma: $T_0^{0^o} \otimes T_1 = IS_0$, $T_0^{120^o} \otimes T_1 = IS_1$ e $T_0^{240^o} \otimes T_1 = IS_2$.

Para construir T_0 e T_1, é necessário que elas sejam divididas em n regiões $R_0, ..., R_{n-1}$. Cada bloco $B_p^{T_0}$ de R_i possui dimensões de $2 \times n$ subpixels, onde $2n-1$ desses subpixels são pretos e somente 1 subpixel é branco. O posicionamento deste subpixel branco é a linha 0 da c-ésima coluna de $B_p^{T_0}$ na R_i, onde $c = i$. Portanto, de acordo com o exemplo anterior, a codificação das imagens secretas IS_0, IS_1 e IS_2 nas transparências T_0 e T_1, implica que os blocos $B_p^{T_0}$ em R_0, R_1 e R_2 sejam construídos de acordo com a TAB. 2.3.

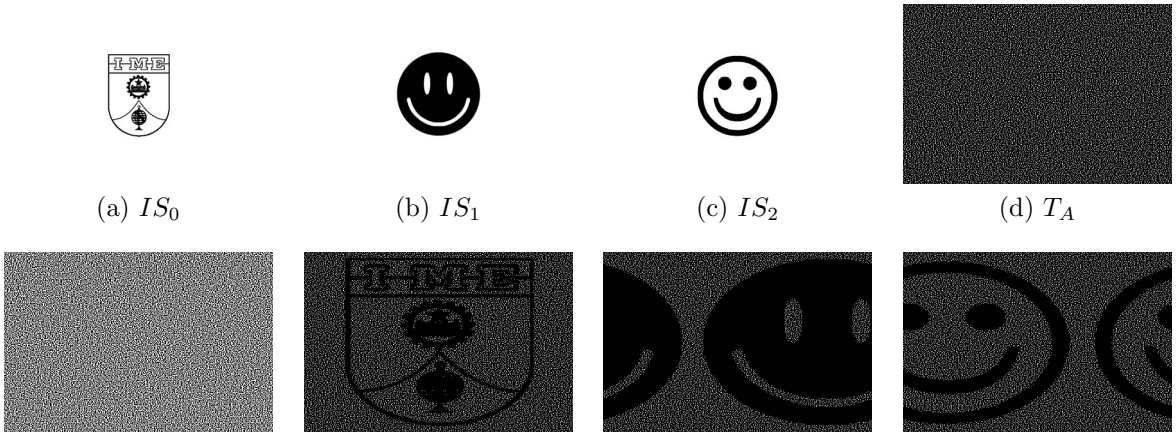
TAB. 2.3: Construções de $B_p^{T_0}$ e $B_p^{T_1}$ no esquema de SHYU et al. (2007).

p-ésimo pixel na IS_x	p-ésimo pixel na IS_y	p-ésimo pixel na IS_z	$B_p^{T_0}$ em R_0	$B_p^{T_0}$ em R_1	$B_p^{T_0}$ em R_2	$B_p^{T_1}$	$B_p^{T_0} + B_p^{T_1}$ em R_0	$B_p^{T_0} + B_p^{T_1}$ em R_1	$B_p^{T_0} + B_p^{T_1}$ em R_2
□	□	□	■□	■□	■□	□■	■□	■□	■□
□	□	■	■□	■□	■□	□■	■□	■□	■■
□	■	□	■□	■□	■□	□■	■□	■■	■□
□	■	■	■□	■□	■□	□■	■□	■■	■■
■	□	□	■□	■□	■□	□■	■■	■□	■□
■	□	■	■□	■□	■□	□■	■■	■□	■■
■	■	□	■□	■□	■□	□■	■■	■■	■□
■	■	■	■□	■□	■□	□■	■■	■■	■■

Cada bloco $B_p^{T_1}$ de R_i também possui dimensões de $2 \times n$ subpixels. Neste caso, metade dos subpixels são pretos e a outra metade dos subpixels são brancos. Cada coluna de um bloco $B_p^{T_1}$ possui um subpixel preto e um subpixel branco. A codificação do p-ésimo pixel de uma das n imagens secretas, definida como IS_j, é determinada pelo posicionamento desses dois subpixels na c-ésima coluna de $B_p^{T_1}$ em R_i, onde $c = i + j \mod n$.

É possível simplificar esta definição, ao verificar sua aplicação na codificação das imagens IS_0, IS_1 e IS_2 em T_0 e T_1, de acordo com a TAB. 2.3. As transparências T_0 e T_1 foram divididas em R_0, R_1 e R_2. Cada coluna c de $B_p^{T_1}$ em R_0 foi codificada considerando $x = 0$, $y = 1$ e $z = 2$. Em R_1, foi definido $x = 2$, $y = 0$ e $z = 1$ para cada coluna de $B_p^{T_1}$. Por fim, cada coluna de $B_p^{T_1}$ em R_2 foi construída considerando $x = 1$, $y = 2$ e $z = 0$.

Para tornar prática esta construção, Alice e Bob devem receber as transparências circulares T_A e T_B, codificadas por três imagens secretas IS_0, IS_1 e IS_2. Eles podem reconstruir IS_0 através da sobreposição $T_A^{0^o} \otimes T_B$, IS_1 através da sobreposição $T_A^{120^o} \otimes T_B$ e IS_2 através da sobreposição $T_A^{240^o} \otimes T_B$. O resultado do experimento que demonstra a construção das transparências e o resultado das sobreposições considerando esta configuração é apresentado na FIG. 2.5.



(a) IS_0 (b) IS_1 (c) IS_2 (d) T_A

(e) T_B (f) $T_A^{0^o} \otimes T_B$ (g) $T_A^{120^o} \otimes T_B$ (h) $T_A^{240^o} \otimes T_B$

FIG. 2.5: Demonstração de $T_A^{0^o} \otimes T_B = IS_0$, $T_A^{120^o} \otimes T_B = IS_1$ e $T_A^{240^o} \otimes T_B = IS_2$.

Na FIG. 2.5, a primeira imagem secreta IS_0 pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS_0. A segunda imagem secreta IS_1 pode ser visualizada no item (b). Foi definido um *smile* de cor predominantemente preta com 150×150 pixels, para ser a IS_1. A terceira imagem secreta IS_2 pode ser visualizada no item (c). Foi definido um *smile* de cor predominantemente branca com 150×150 pixels, para ser a IS_2.

As duas transparências circulares T_A e T_B, que podem ser visualizadas nos itens (d) e (e), respectivamente, foram construídas a partir de IS_0, IS_1 e IS_2. As transparências circulares T_A e T_B possuem 300×450 pixels. As sobreposições $T_A^{0^o} \otimes T_B$, $T_A^{120^o} \otimes T_B$ e $T_A^{240^o} \otimes T_B$, que podem ser visualizadas nos itens (f), (g) e (h), definem as reconstruções de IS_0, IS_1 e IS_2, respectivamente.

2.6 SEGURANÇA EM CRIPTOGRAFIA VISUAL

Neste Capítulo foi possível verificar alguns esquemas de Criptografia Visual, mais especificamente na Seção 2.4 e na Seção 2.5. Através das definições e demonstrações apresentadas, tornou-se possível concluir que suas características estão em concordância com o conjunto de requisitos que define um sistema perfeito, de acordo com as definições de SHANNON (1949), que foram apresentadas na Seção 2.3.

De fato, NAOR e SHAMIR (1996) afirmaram que um sistema criptográfico baseado no $(k, n)VCS$ fornece a segurança incondicional dos sistemas perfeitos. No entanto, HORNG, CHEN e TSAI (2006) demonstraram que um $(k, n)VCS$ com $k = 2$ e $n > 2$ é inseguro contra a fraude introduzida por TOMPA e WOLL (1989) sobre um $(k, n)TS$. HORNG, CHEN e TSAI (2006) demonstraram que $n - 1$ participantes desonestos podem trabalhar em conjunto com o objetivo de fraudar a imagem secreta. Desta forma, eles se tornariam capazes de enganar um participante honesto. A fraude em Criptografia Visual será apresentada no Capítulo 3.

3 FRAUDE EM CRIPTOGRAFIA VISUAL

O objetivo deste Capítulo é apresentar o método de execução da fraude em Criptografia Visual demonstrado por HORNG, CHEN e TSAI (2006), cuja introdução foi realizada por TOMPA e WOLL (1989) sobre um $(k, n)TS$. A fraude será realizada sobre um $(2, n > 2)VCS$. Este Capítulo está organizado da seguinte forma. Na Seção 3.1 serão apresentadas as definições sobre a estrutura de um $(2, n > 2)VCS$. Um experimento realizado demonstra a construção e a sobreposição das transparências em um $(2, 3)VCS$. Na Seção 3.2, o conceito sobre fraude no $(2, n > 2)VCS$ será introduzido, através de uma descrição detalhada sobre a construção das transparências falsas. Na Seção 3.3 será demonstrado, através de outro experimento, a execução com sucesso da fraude no $(2, 3)VCS$. O Capítulo será concluído na Seção 3.4 através de uma breve análise sobre a prevenção contra a fraude demonstrada.

3.1 CONSTRUÇÃO DE UM $(2, N)VCS$

Uma construção especial em Criptografia Visual foi definida por NAOR e SHAMIR (1995) como $(2, n)VCS$. Nesta estrutura, as duas matrizes S_0 e S_1 possuem dimensões $n \times m$, onde $m = n$, e são construídas da seguinte forma: a matriz S_0 possui o valor 1 em todas as posições da primeira coluna e o valor 0 nas posições referentes às outras colunas; e a matriz S_1 possui o valor 1 em todas as posições de sua diagonal principal e o valor 0 nas outras posições.

$$S_0 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}; S_1 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Assim como foi descrito na Seção 2.4, as coleções C_0 e C_1 são formadas pelas matrizes obtidas através de todas as permutações possíveis das colunas de S_0 e S_1. Para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel da imagem secreta IS for branco, o esquema escolhe aleatoriamente uma das matrizes em C_0, e para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel da imagem secreta IS for preto, o esquema escolhe aleatoriamente uma das matrizes

em C_1. Neste trabalho, será utilizada a construção de um $(2,3)VCS$ como base para a realização dos próximos experimentos. As duas matrizes S_0 e S_1 são definidas em um $(2,3)VCS$ de acordo com a construção definida para um $(2,n)VCS$. Os parâmetros utilizados serão $m = 3$ e $\alpha = \frac{1}{2}$.

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}; S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

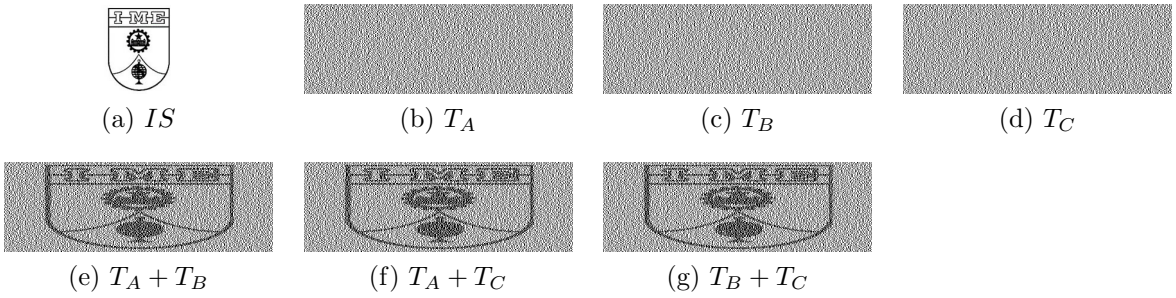
Os participantes convidados serão Alice, Bob e Carol. Eles devem receber as transparências T_A, T_B e T_C, respectivamente. As construções dos blocos $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ são baseadas nas escolhas aleatórias das coleções C_0 e C_1, de acordo com a cor do p-ésimo pixel da imagem secreta IS. Todas as possíveis construções dos blocos $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ podem ser visualizadas na TAB. 3.1.

TAB. 3.1: Construções de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ em um $(2,3)VCS$ com $m = 3$.

Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A} + B_p^{T_B}$	$B_p^{T_A} + B_p^{T_C}$	$B_p^{T_B} + B_p^{T_C}$
1	□	■□□	■□□	■□□	■□□	■□□	■□□
	□	□■□	□■□	□■□	□■□	□■□	□■□
	□	□□■	□□■	□□■	□□■	□□■	□□■
2	■	■□□	■□□	□□■	■□□	■□□	□■□
	■	■□□	□□■	□■□	■□□	■□□	□■□
	■	□■□	■□□	□□■	■□□	□■□	■□□
	■	□□■	■□□	□■□	■□□	□■□	■□□
	■	□■□	□□■	■□□	□■□	■□□	■□□
	■	□□■	□■□	■□□	□■□	■□□	■□□

No primeiro caso da TAB. 3.1, o p-ésimo pixel da imagem secreta IS é branco. Ele pode ser codificado de três formas diferentes, com probabilidade $\frac{1}{3}$ de ocorrência , expandido nos blocos $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$, que se equivalem nos blocos resultantes das sobreposições $B_p^{T_A} + B_p^{T_B}$, $B_p^{T_A} + B_p^{T_C}$ e $B_p^{T_B} + B_p^{T_C}$. No segundo caso da TAB. 3.1, o p-ésimo pixel da imagem

secreta IS é preto. Ele pode ser codificado de seis formas diferentes, com probabilidade $\frac{1}{6}$ de ocorrência, expandido nos blocos $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$, que se complementam nos blocos resultantes das sobreposições $B_p^{T_A} + B_p^{T_B}$, $B_p^{T_A} + B_p^{T_C}$ e $B_p^{T_B} + B_p^{T_C}$. O resultado do experimento é apresentado na FIG. 3.1.



(a) IS (b) T_A (c) T_B (d) T_C

(e) $T_A + T_B$ (f) $T_A + T_C$ (g) $T_B + T_C$

FIG. 3.1: Demonstração de $T_A + T_B = IS$, $T_A + T_C = IS$ e $T_B + T_C = IS$ no $(2, 3)VCS$.

Na FIG. 3.1, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. As três transparências T_A, T_B e T_C, que podem ser visualizadas nos itens (b), (c) e (d), respectivamente, foram construídas a partir da IS. Cada T_i possui 150×450 pixels. As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas itens (e), (f) e (g), respectivamente, definem as reconstruções da IS.

3.2 DEFINIÇÕES SOBRE FRAUDE EM UM $(2, N > 2)VCS$

A segurança do esquema de SHAMIR (1979) foi violada por TOMPA e WOLL (1989), quando eles afirmaram que existe a possibilidade de que quaisquer $k - 1$ participantes $P_1, ..., P_{k-1}$ possam construir novas partes $D'_1, ..., D'_{k-1}$ com o objetivo de enganar o k-ésimo participante P_k. Determinar que P_k foi enganado significa concluir que o dado secreto D', reconstruído pela junção entre as partes falsas $D'_1, ..., D'_{k-1}$ e a parte original D_k, foi considerado legal, apesar de ser incorreto, pois $D \neq D'$. Esta definição sobre fraude foi aplicada no contexto da Criptografia Visual por HORNG, CHEN e TSAI (2006). O fluxograma de execução da fraude é apresentado na FIG. 3.2.

De acordo com HORNG, CHEN e TSAI (2006), os participantes de um $(2, n)VCS$, $P_0, ..., P_{n-2}$ são capazes de se reunir com o objetivo de construir transparências falsas $T'_0, ..., T'_{n-2}$, e assim enganar o participante P_{n-1} durante o processo de sobreposição entre a sua transparência original T_{n-1} e qualquer uma das transparências falsas $T'_0, ..., T'_{n-2}$.

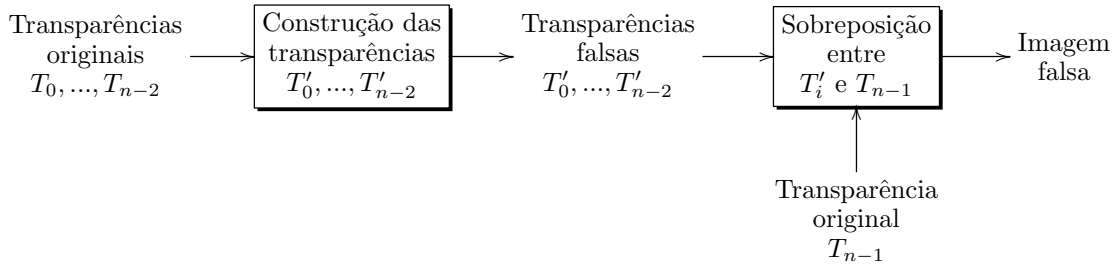


FIG. 3.2: Fluxo para a construção de $T'_0, ..., T'_{n-2}$ em um $(2, n)VCS$.

Neste cenário, Alice, Bob e Carol devem receber as transparências T_A, T_B e T_C, respectivamente. Supondo que o desejo de Alice e Bob seja enganar Carol, então eles devem construir suas transparências falsas T'_A e T'_B através das transformações de $B_p^{T_A}$ em $B_p^{T'_A}$, denotada por $B_p^{T_A} \rightarrow B_p^{T'_A}$ e de $B_p^{T_B}$ em $B_p^{T'_B}$, denotada por $B_p^{T_B} \rightarrow B_p^{T'_B}$, com base no bloco $B_p^{T_C}$ que Alice e Bob são capazes de prever. Cada transformação deve ser realizada com base no p-ésimo pixel da IS.

A imagem falsa IF será reconstruída quando as transparências falsas de Alice e Bob T'_A e T'_B forem sobrepostas com a transparência original de Carol T_C. Na TAB. 3.2, são apresentadas todas as possibilidades de transformação, caso o p-ésimo pixel da imagem secreta IS seja branco.

TAB. 3.2: Transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ caso o p-ésimo pixel seja branco.

Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	p-ésimo pixel na IF	$B_p^{T'_A}$	$B_p^{T'_B}$
1	□	■□	■□	■□	□	■□	■□
	□	□■	□■	□■	□	□■	□■
	□	□■	□■	□■	□	□■	□■
2	□	■□	■□	■□	■	□■	□■
	□	■□	■□	■□	■	□■	□■
	□	□■	□■	□■	■	■□	□■
	□	□■	□■	□■	■	□■	■□
	□	□■	□■	□■	■	■□	□■
	□	□■	□■	□■	■	□■	■□

No primeiro caso da TAB. 3.2, $B_p^{T_A}$ será igual a $B_p^{T'_A}$, ou $B_p^{T_A} = B_p^{T'_A}$ e $B_p^{T_B}$ será igual a $B_p^{T'_B}$, ou $B_p^{T_B} = B_p^{T'_B}$, pois o p-ésimo pixel da IS é igual ao p-ésimo pixel da IF. No segundo caso da TAB. 3.2, Alice e Bob devem comparar $B_p^{T_A}$ e $B_p^{T_B}$ e inferir sobre $B_p^{T_C}$, pois o p-ésimo pixel da IS é branco e o p-ésimo pixel da IF é preto. Eles devem realizar as transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ para que o bloco resultante de cada sobreposição $B_p^{T'_A} + B_p^{T_C}$ e $B_p^{T'_B} + B_p^{T_C}$ seja preto. Na TAB. 3.3 são apresentadas todas as possibilidades de transformação, caso o p-ésimo pixel da imagem secreta IS seja preto.

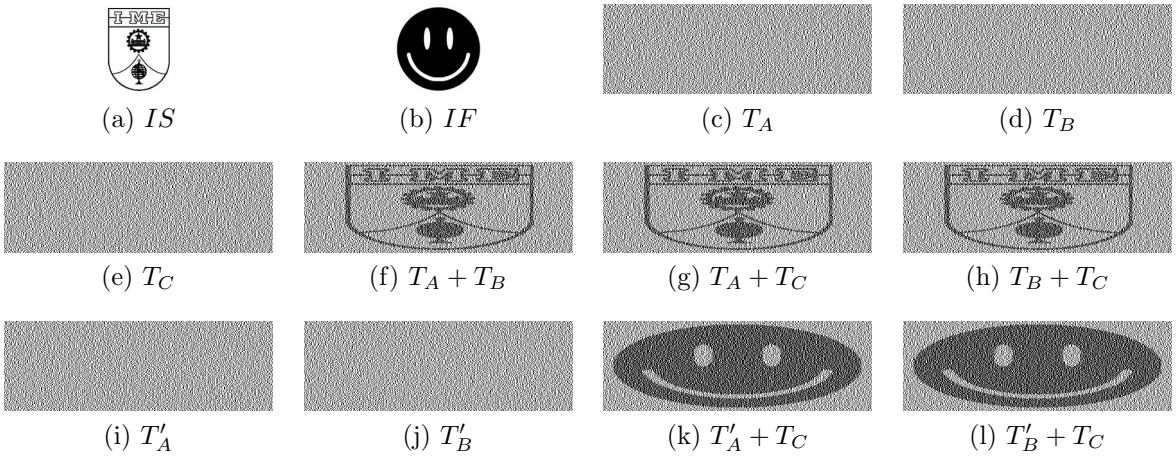
TAB. 3.3: Transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ caso o p-ésimo pixel seja preto.

Caso	p-ésimo pixel na IS	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	p-ésimo pixel na IF	$B_p^{T'_A}$	$B_p^{T'_B}$
1	■	■□	■□	■□	□	□■	□■
	■	□■	■□	□■	□	□■	□■
	■	■□	□■	■□	□	□■	□■
	■	□■	■□	■□	□	□■	□■
	■	□■	□■	■□	□	■□	■□
	■	□■	■□	□■	□	■□	■□
2	■	■□	□■	□■	■	■□	□■
	■	□■	■□	□■	■	□■	■□
	■	■□	□■	■□	■	■□	□■
	■	□■	■□	■□	■	□■	■□
	■	□■	□■	□■	■	□■	□■
	■	□■	■□	■□	■	□■	■□

No primeiro caso da TAB. 3.3, Alice e Bob devem comparar $B_p^{T_A}$ e $B_p^{T_B}$ e inferir sobre $B_p^{T_C}$, pois o p-ésimo pixel da IS é preto e o p-ésimo pixel da IF é branco. Eles devem realizar as transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ para que o bloco resultante de cada sobreposição $B_p^{T'_A} + B_p^{T_C}$ e $B_p^{T'_B} + B_p^{T_C}$ seja branco. No segundo caso da TAB. 3.3, $B_p^{T_A} = B_p^{T'_A}$ e $B_p^{T_B} = B_p^{T'_B}$, pois o p-ésimo pixel da IS é igual ao p-ésimo pixel da IF.

3.3 EXECUÇÃO DA FRAUDE EM UM $(2,3)VCS$

A construção definida na Seção 3.2 constitui a base necessária para a realização do experimento que demonstra a fraude em um $(2,3)VCS$. Alice, Bob e Carol devem receber as transparências T_A, T_B e T_C, respectivamente. Os parâmetros utilizados serão $m = 3$ e $\alpha = \frac{1}{2}$, os mesmos definidos na Seção 3.1. Supondo que o desejo de Alice e Bob seja enganar Carol, então eles deverão construir T'_A e T'_B através das transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$, de acordo com as definições apresentadas na Seção 3.2, quando o p-ésimo pixel da IS for diferente do p-ésimo pixel da IF. O resultado deste experimento pode ser visualizado na FIG. 3.3.



(a) IS (b) IF (c) T_A (d) T_B

(e) T_C (f) $T_A + T_B$ (g) $T_A + T_C$ (h) $T_B + T_C$

(i) T'_A (j) T'_B (k) $T'_A + T_C$ (l) $T'_B + T_C$

FIG. 3.3: Demonstração de $T'_A + T_C = IF$ e $T'_B + T_C = IF$ no $(2,3)VCS$.

Na FIG. 3.3, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem falsa IF escolhida por Alice e Bob pode ser visualizada no item (b). Foi definido um *smile* de cor predominantemente preta com 150×150 pixels, para ser a IF. As três transparências originais T_A, T_B e T_C podem ser visualizadas nos itens (c), (d) e (e), respectivamente. A construção de T_A, T_B e T_C foi realizada a partir de IS com base no $(2,3)VCS$. Cada T_i possui 150×450 pixels.

As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (f), (g) e (h), respectivamente, definem as reconstruções da IS. As duas transparências falsas T'_A e T'_B, que podem ser visualizadas nos itens (i) e (j), respectivamente, foram construídas a partir da IF. Cada T'_i também possui 150×450 pixels. As sobreposições $T'_A + T_C$ e $T'_B + T_C$, que podem ser visualizadas nos itens (k) e (l), respectivamente, definem as reconstruções da IF.

3.4 PREVENÇÃO CONTRA FRAUDE EM CRIPTOGRAFIA VISUAL

Na Seção 3.3 foi demonstrada a execução com sucesso da fraude. Afirmar que Carol foi enganada significa concluir que a imagem falsa, reconstruída a partir das sobreposições $T'_A + T_C$ e $T'_B + T_C$ foi considerada autêntica, apesar de ser incorreta, pois $IS \neq IF$. No entanto, é possível que Carol evite a fraude, se ela for capaz de suspeitar que as transparências apresentadas por Alice e Bob não são originais ou que a imagem reconstruída após as sobreposições não é verdadeira.

De acordo com HORNG, CHEN e TSAI (2006), a solução natural para o problema da fraude deve ser obtida através do conceito de autenticação em Criptografia Visual, introduzido por NAOR e PINKAS (1997). Esquemas deste tipo são conhecidos como $ABCPS$. Eles forneceriam a Carol, a capacidade de verificar a integridade das transparências T_A, T'_A, T_B ou T'_B antes de reconstruir a IS ou IF através das sobreposições $T_A + T_C$, $T'_A + T_C$, $T_B + T_C$ ou $T'_B + T_C$.

Os dois principais esquemas de prevenção contra fraude são do tipo $ABCPS$ e foram criados por HORNG, CHEN e TSAI (2006) e HU e TZENG (2007). Neste trabalho, esses esquemas serão chamados de HCT e HT, respectivamente, como referências às iniciais dos seus criadores. No Capítulo 4, esses esquemas serão apresentados, assim como os seus mecanismos de segurança e as suas vulnerabilidades relacionadas.

4 ESQUEMAS DE PREVENÇÃO CONTRA FRAUDE

O objetivo deste Capítulo é apresentar os dois principais esquemas de prevenção contra a fraude demonstrada no Capítulo 3, além de fornecer uma análise sobre os ataques realizados sobre eles, com base na demonstração através de experimentos das vulnerabilidades identificadas e na apresentação de sugestões sobre possíveis correções aos esquemas, formando a base para a construção de um novo esquema de prevenção contra fraude em Criptografia Visual. Este Capítulo está organizado da seguinte forma. Na Seção 4.1 será apresentada a estrutura do esquema HCT, desenvolvido por HORNG, CHEN e TSAI (2006), além de um experimento que demonstra o mecanismo de prevenção associado ao esquema. Na Seção 4.2, a primeira vulnerabilidade do HCT, que foi identificada por HU e TZENG (2007), será demonstrada, através de um experimento que simula o ataque ao esquema. Na Seção 4.3, a segunda vulnerabilidade do HCT, que foi identificada por LIU, WU e LIN (2011), será demonstrada, através de três experimentos que simulam diferentes ataques ao esquema, e comprovam que o sucesso deste ataque pode ser atingido mediante o cumprimento de alguns pré-requisitos. Na Seção 4.4, será apresentada a estrutura do esquema HT, desenvolvido por HU e TZENG (2007), além de um experimento que demonstra o mecanismo de prevenção relacionado ao esquema. Na Seção 4.5, a vulnerabilidade do HT, que foi identificada por LIU, WU e LIN (2011), será demonstrada, através de um experimento que simula o ataque ao esquema. O Capítulo será concluído na Seção 4.6, através de uma análise sobre as vulnerabilidades relacionadas aos esquemas HCT e HT, com base em um conjunto de correções relevantes aos aspectos de segurança para o projeto de um novo esquema de prevenção contra fraude em Criptografia Visual.

4.1 PREVENÇÃO HCT

O esquema de prevenção HCT é um $ABCPS$ desenvolvido por HORNG, CHEN e TSAI (2006). A estrutura básica deste esquema é apresentada no fluxograma da FIG. 4.1. Nele, os participantes $P_0, ..., P_{n-1}$ recebem transparências originais $T_0, ..., T_{n-1}$ e transparências extras de verificação $V_0, ..., V_{n-1}$. Cada T_i é construída por um $(k, n)VCS$. A transparência de verificação V_i é utilizada para verificar a integridade de cada transparência T_j, onde $j = 0, ..., n-1$, e $j \neq i$.

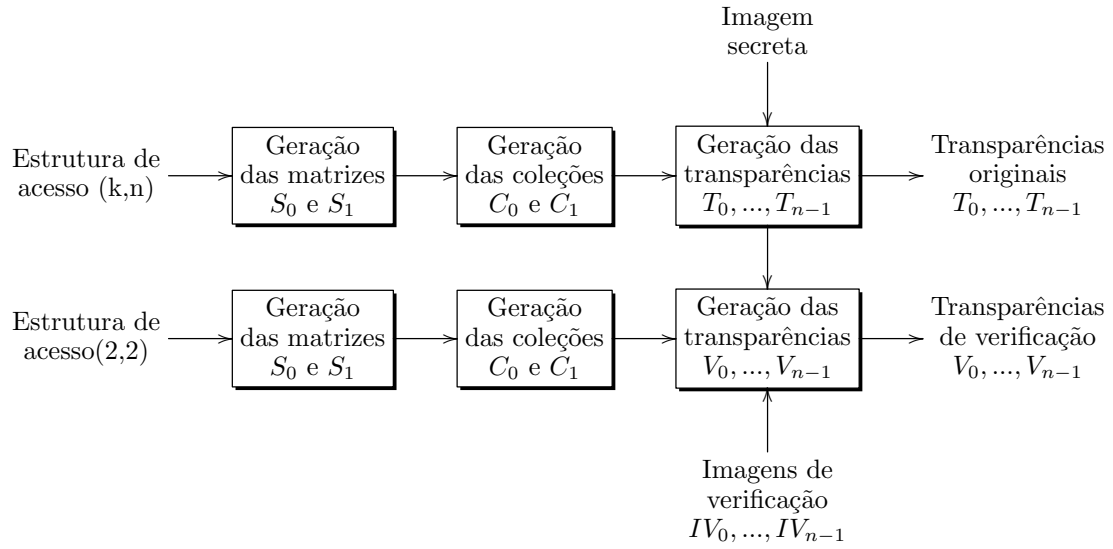


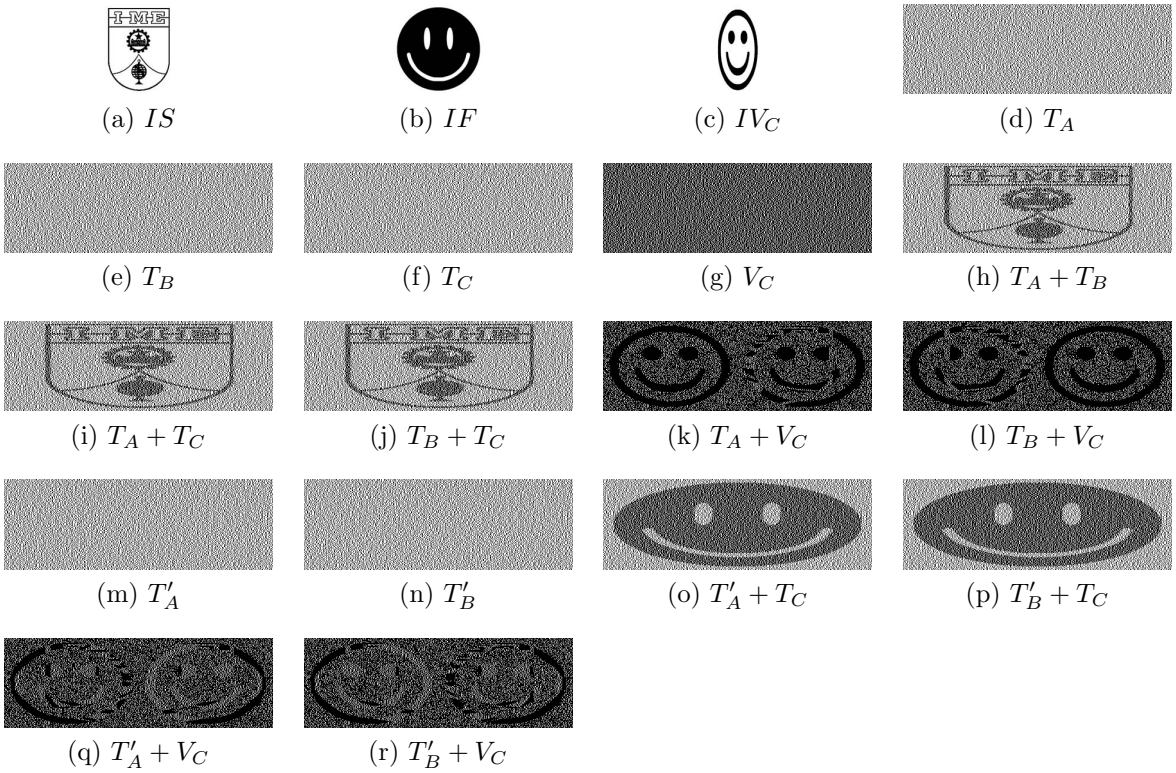
FIG. 4.1: Fluxo para a construção de $T_0, ..., T_{n-1}$ e $V_0, ..., V_{n-1}$ no HCT. Adaptação: (CIMATO e YANG, 2011).

Cada participante P_i deve enviar ao esquema, através de canais seguros, uma imagem de verificação IV_i para ser autenticada durante a verificação de integridade das transparências dos outros participantes. A construção de $T_0, ..., T_{n-1}$ é baseada em um $(k, n)VCS$, e a construção de $V_0, ..., V_{n-1}$ é baseada em um $(2, 2)VCS$. Cada V_i é dividida em $n-1$ regiões R_{ij}, onde $0 \leq j \leq n-1$ e $j \neq i$. A sobreposição $V_i + T_j$ deve reconstruir IV_i na região R_{ij}.

Portanto, ao utilizar o HCT, Alice, Bob e Carol recebem, além de T_A, T_B e T_C, as transparências V_A, V_B e V_C, respectivamente. Carol é capaz de verificar a integridade de T_A e T_B através de V_C. HORNG, CHEN e TSAI (2006) definiram que o processo é composto pelas fases de inicialização, autenticação e decodificação.

Na inicialização, Alice, Bob e Carol escolhem individualmente IV_A, IV_B e IV_C e as enviam com segurança ao sistema. Em seguida, na fase de autenticação, Carol sobrepõe V_C com T_A ou com T_B. Caso IV_C não seja reconstruída em alguma região de V_C, Carol deve rejeitar a transparência do outro participante. Por outro lado, se a autenticação de IV_C for efetuada com sucesso, Carol pode realizar a sobreposição $T_C + T_A$ ou $T_C + T_B$ e concluir a fase de decodificação.

Como os participantes supostamente desonestos Alice e Bob não conhecem IV_C, então a probabilidade de que eles possam construir T'_A e T'_B que sejam aprovadas pela verificação de Carol, realizada por $V_C + T'_A$ e $V_C + T'_B$ foi descartada por HORNG, CHEN e TSAI (2006). O resultado do experimento é apresentado na FIG. 4.2.



(a) IS (b) IF (c) IV_C (d) T_A

(e) T_B (f) T_C (g) V_C (h) $T_A + T_B$

(i) $T_A + T_C$ (j) $T_B + T_C$ (k) $T_A + V_C$ (l) $T_B + V_C$

(m) T'_A (n) T'_B (o) $T'_A + T_C$ (p) $T'_B + T_C$

(q) $T'_A + V_C$ (r) $T'_B + V_C$

FIG. 4.2: Demonstração de $T'_A + V_C \neq IV_C$ e $T'_B + V_C \neq IV_C$ no HCT.

Na FIG. 4.2, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem falsa IF escolhida por Alice e Bob pode ser visualizada no item (b). Foi definido um *smile* de cor predominantemente preta com 150×150 pixels, para ser a IF. A imagem de verificação IV_C escolhida por Carol pode ser visualizada no item (c). Foi definido um *smile* de cor predominantemente branca com 150×75 pixels, para ser a IV_C.

As três transparências originais T_A, T_B e T_C, que podem ser visualizadas nos itens (d), (e) e (f), respectivamente, foram construídas a partir de IS. Cada T_i possui 150×450 pixels. A transparência de verificação de Carol V_C, que pode ser visualizada no item (g), foi construída a partir de IV_C. Esta transparência também possui 150×450 pixels.

As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (h), (i) e (j), respectivamente, definem as reconstruções de IS. As sobreposições $T_A + V_C$ e $T_B + V_C$, que podem ser visualizadas nos itens (k) e (l), definem as reconstruções de IV_C em R_{CA} e R_{CB}, respectivamente. As duas transparências falsas T'_A e T'_B, que podem ser visualizadas nos itens (m) e (n), respectivamente, foram construídas a partir de IF.

As sobreposições $T'_A + T_C$ e $T'_B + T_C$, que podem ser visualizadas nos itens (o) e (p), respectivamente, definem as reconstruções de IF. As sobreposições $T'_A + V_C$ e $T'_B + V_C$, que podem ser visualizadas nos itens (q) e (r), não definem com clareza a reconstrução de IV_C em R_{CA} e R_{CB}, respectivamente. Cada T'_i também possui 150×450 pixels.

4.2 PRIMEIRO ATAQUE AO HCT: V_I VERIFICA PARCIALMENTE A INTEGRIDADE DE T_J

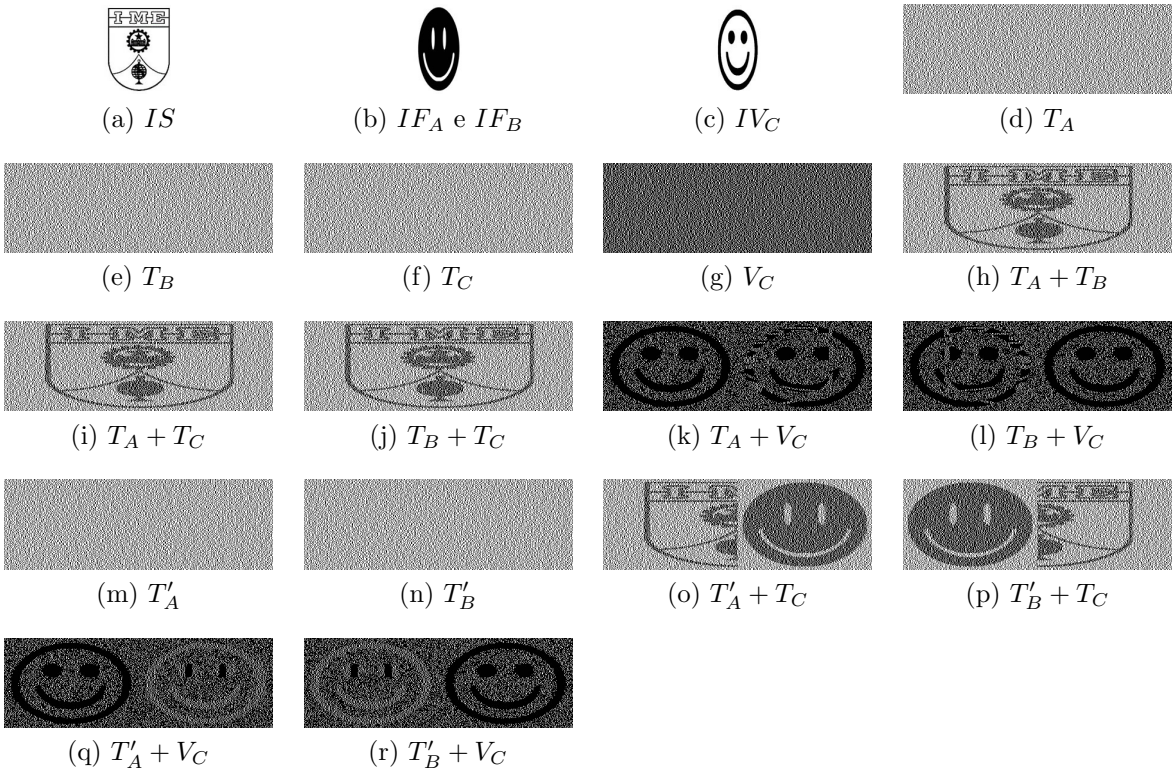
O primeiro ataque ao esquema HCT foi realizado por HU e TZENG (2007). Eles definiram que, caso um participante qualquer P_j conheça a localização de R_{ij} em V_i, onde $j \neq i$, então P_j será capaz de criar T'_j, de forma que, caso $B_p^{T_j}$ possua localização correspondente a R_{ij}, então $B_p^{T_j} = B_p^{T'_j}$, e caso $B_p^{T_j}$ não possua localização correspondente a R_{ij}, então a construção de $B_p^{T'_j}$ poderá ser realizada com base na IF, de acordo com transformação $B_p^{T_j} \rightarrow B_p^{T'_j}$, definida na Seção 3.2. Desta forma, P_i autenticará a IV_i reconstruída em R_{ij} após a verificação $T'_j + V_i$ e deverá acreditar que T'_j é verdadeira.

É possível assumir que os participantes supostamente desonestos Alice e Bob estejam dispostos a realizar este ataque. Se Alice descobrir a localização de R_{CA} na transparência de verificação V_C, então ela será capaz de construir sua transparência falsa T'_A, de forma que, caso $B_p^{T_A}$ possua localização correspondente a R_{CA}, então $B_p^{T_A} = B_p^{T'_A}$, e caso $B_p^{T_A}$ não possua localização correspondente a R_{CA}, então $B_p^{T_A} \rightarrow B_p^{T'_A}$.

De forma semelhante, se Bob descobrir a localização de R_{CB} na transparência de verificação V_C, então ele será capaz de construir sua transparência falsa T'_B, de forma que, caso $B_p^{T_B}$ possua localização correspondente a R_{CB}, então $B_p^{T_B} = B_p^{T'_B}$, e caso $B_p^{T_B}$ não possua localização correspondente a R_{CB}, então $B_p^{T_B} \rightarrow B_p^{T'_B}$.

Para realizar este ataque, Alice e Bob não precisam trabalhar em conjunto. Em qualquer um dos casos, Carol autenticará a IV_C reconstruída em R_{CA} ou R_{CB}, após as verificações $T'_A + V_C$ ou $T'_B + V_C$, e será enganada por Alice ou Bob ao acreditar na autenticidade de T'_A ou T'_B.

O único requisito que Alice e Bob devem atingir para obter sucesso na realização deste ataque está relacionado com a descoberta da localização das regiões R_{CA} e R_{CB} que codificaram as partes de T_A e T_B, respectivamente, na transparência de verificação V_C. Em um $(2, 3)VCS$, a probabilidade de sucesso nesta descoberta é de $\frac{1}{2}$. O resultado de um experimento que demonstra o ataque realizado por Alice e Bob sobre esta vulnerabilidade do HCT é apresentado na FIG. 4.3.



(a) IS (b) IF_A e IF_B (c) IV_C (d) T_A

(e) T_B (f) T_C (g) V_C (h) $T_A + T_B$

(i) $T_A + T_C$ (j) $T_B + T_C$ (k) $T_A + V_C$ (l) $T_B + V_C$

(m) T'_A (n) T'_B (o) $T'_A + T_C$ (p) $T'_B + T_C$

(q) $T'_A + V_C$ (r) $T'_B + V_C$

FIG. 4.3: Demonstração de $T'_A + V_C = IV_C$ e $T'_B + V_C = IV_C$ no HCT com modificação parcial de T_A e T_B.

Na FIG. 4.3, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem falsa IF escolhida por Alice e Bob pode ser visualizada no item (b). Foi definido um *smile* de cor predominantemente preta com 150×75 pixels, para ser a IF. A imagem de verificação IV_C escolhida por Carol pode ser visualizada no item (c). Foi definido um *smile* de cor predominantemente branca com 150×75 pixels, para ser a IV_C.

As três transparências originais T_A, T_B e T_C, que podem ser visualizadas nos itens (d), (e) e (f), respectivamente, foram construídas a partir de IS. Cada T_i possui 150×450 pixels. A transparência de verificação de Carol V_C, que pode ser visualizada no item (g), foi construída a partir de IV_C. Esta transparência também possui 150×450 pixels.

As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (h), (i) e (j), respectivamente, definem as reconstruções de IS. As sobreposições $T_A + V_C$ e $T_B + V_C$, que podem ser visualizadas nos itens (k) e (l), definem as reconstruções de IV_C em R_{CA} e R_{CB}, respectivamente.

As duas transparências falsas T'_A e T'_B, que podem ser visualizadas nos itens (m) e (n), respectivamente, foram construídas a partir de IF. Cada T'_i também possui 150×450 pixels. As sobreposições $T'_A + T_C$ e $T'_B + T_C$, que podem ser visualizadas nos itens (o) e (p), definem as reconstruções de IF fora de R_{CA} (em R_{CB}) e fora de R_{CB} (em R_{CA}), respectivamente. As sobreposições $T'_A + V_C$ e $T'_B + V_C$, que podem ser visualizadas nos itens (q) e (r), definem as reconstruções de IV_C em R_{CA} e R_{CB}, respectivamente.

4.3 SEGUNDO ATAQUE AO HCT: P_I OBTÉM IS INDIVIDUALMENTE

O segundo ataque ao esquema HCT foi realizado por LIU, WU e LIN (2011). A vulnerabilidade que este ataque explora afeta a confidencialidade da IS, pois demonstra que qualquer participante é capaz reconstruí-la individualmente. Trata-se de uma falha mais grave que a identificada por HU e TZENG (2007), e descrita na Seção 4.2.

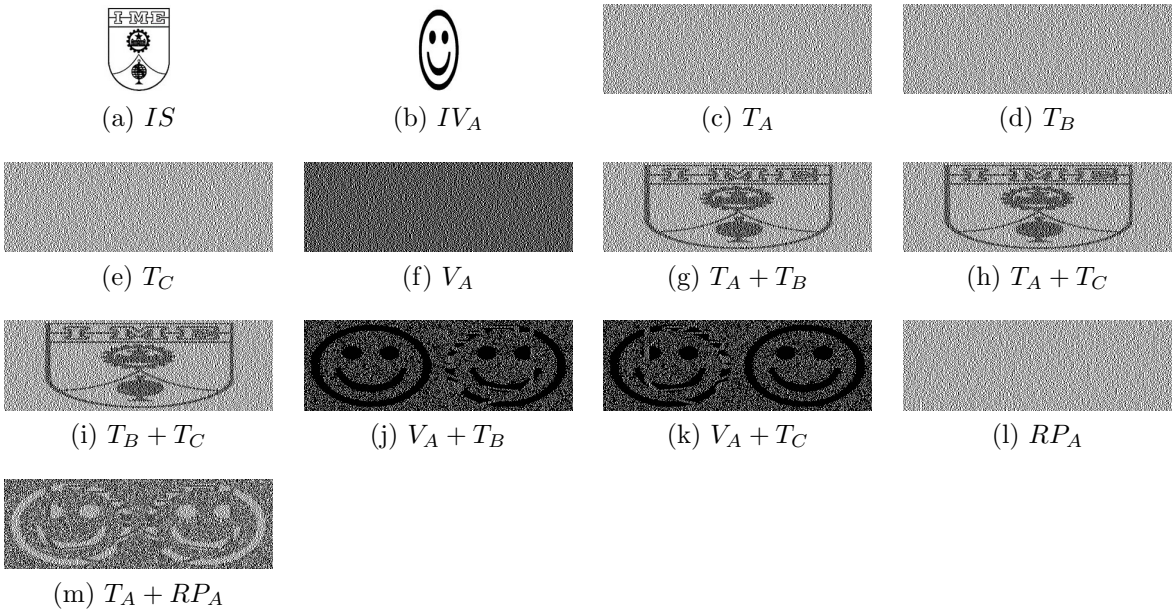
Sabe-se que P_i possui T_i e V_i, e conhece IV_i. Cada T_j foi codificada com V_i por um $(2,2)VCS$ na região R_{ij}, sendo IV_i a imagem utilizada nesta codificação. Portanto, é possível afirmar que P_i é capaz de reconstruir a parte de T_j correspondente a R_{ij}, a partir de V_i e IV_i. A sobreposição desta reconstrução parcial com T_i revela em R_{ij}, parte da IS. A repetição do processo para as $n-2$ regiões em V_i permitirá que o participante P_i recupere IS individualmente.

Esta vulnerabilidade é muito interessante, tanto para Alice quanto para Bob, que são os participantes desonestos. Por exemplo, é possível assumir que Alice realize este ataque. Ela possui T_A e V_A, e conhece IV_A. Sabe-se que parte de T_B e de T_C foram codificadas com V_A por um $(2,2)VCS$ em R_{AB} e R_{AC}, respectivamente, e que IV_A é a imagem utilizada nesta codificação. Então, Alice é capaz de reconstruir as partes de T_B e T_C, correspondentes a R_{AB} e R_{AC}, respectivamente, a partir de V_A e IV_A.

De forma semelhante, Bob também poderia recuperar a IS individualmente, pois ele possui T_B e V_B, e conhece IV_B. Sabe-se que parte de T_A e de T_C foram codificadas com V_B por um $(2,2)VCS$ em R_{BA} e R_{BC}, respectivamente, e que IV_B é a imagem utilizada nesta codificação. Então, Bob poderia reconstruir as partes de T_A e T_C, correspondentes a R_{BA} e R_{BC}, respectivamente, a partir de V_B e IV_B.

Nos experimentos demonstrados nesta Seção, Alice será a participante desonesta que tentará recuperar a IS individualmente. Após realizar o ataque, espera-se que a sobreposição da reconstrução parcial de T_B com T_A revele a metade da IS em R_{AB} e que a sobreposição da reconstrução parcial de T_C com T_A revele em R_{AC} a outra metade da IS.

A transparência construída por Alice, que é composta pela concatenação das reconstruções parciais de T_B e T_C correspondentes a R_{AB} e R_{AC}, respectivamente, será nomeada como RP_A. Desta forma, o ataque será concluído quando Alice realizar a sobreposição $T_A + RP_A$. Três experimentos que demonstram a exploração desta vulnerabilidade no HCT são apresentados na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6.



(a) IS (b) IV_A (c) T_A (d) T_B

(e) T_C (f) V_A (g) $T_A + T_B$ (h) $T_A + T_C$

(i) $T_B + T_C$ (j) $V_A + T_B$ (k) $V_A + T_C$ (l) RP_A

(m) $T_A + RP_A$

FIG. 4.4: Demonstração de $T_A + RP_A \neq IS$ no HCT com IV_A predominantemente branca.

Na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem de verificação IV_A escolhida por Alice pode ser visualizada no item (b).

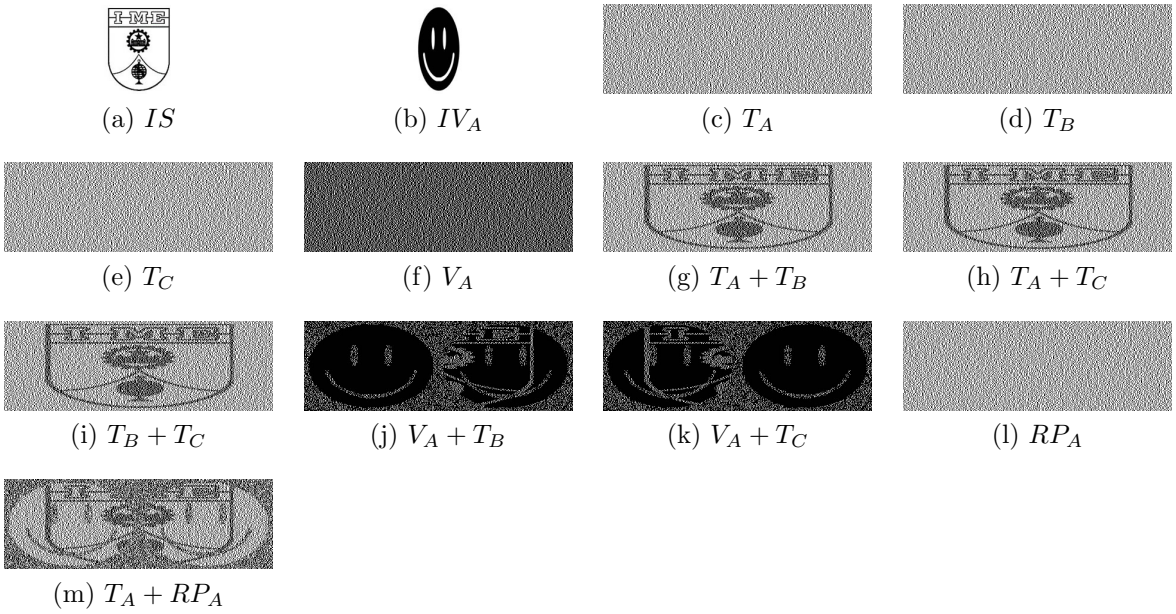
As três transparências originais T_A, T_B e T_C, que podem ser visualizadas nos itens (c), (d) e (e), respectivamente, foram construídas a partir de IS. Cada T_i possui 150×450 pixels. A transparência de verificação de Alice V_A, que pode ser visualizada no item (f), foi construída a partir de IV_A. Esta transparência também possui 150×450 pixels.

As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (g), (h) e (i), respectivamente, definem as reconstruções de IS. As sobreposições $V_A + T_B$ e $V_A + T_C$, que podem ser visualizadas nos itens (j) e (k), definem as reconstruções de IV_A em R_{AB} e R_{AC}, respectivamente.

A transparência RP_A, que pode ser visualizada no item (l), é composta pela concatenação das reconstruções parciais realizadas por Alice das transparências T_B e T_C,

correspondentes às regiões R_{AB} e R_{AC}, respectivamente. A sobreposição $T_A + RP_A$ pode ser visualizada no item (m).

A principal diferença entre os experimentos demonstrados na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6 é a definição da imagem de verificação escolhida por Alice, que interfere nos resultados dos ataques. No primeiro experimento, que foi demonstrado na FIG. 4.4, Alice escolheu um *smile* de cor predominantemente branca para ser a IV_A. No segundo experimento, que foi demonstrado na FIG. 4.5, ela escolheu um *smile* de cor predominantemente preta para ser a IV_A. No último experimento, que foi demonstrado na FIG. 4.6, a escolha de Alice foi uma imagem completamente preta para ser a IV_A.



(a) IS (b) IV_A (c) T_A (d) T_B

(e) T_C (f) V_A (g) $T_A + T_B$ (h) $T_A + T_C$

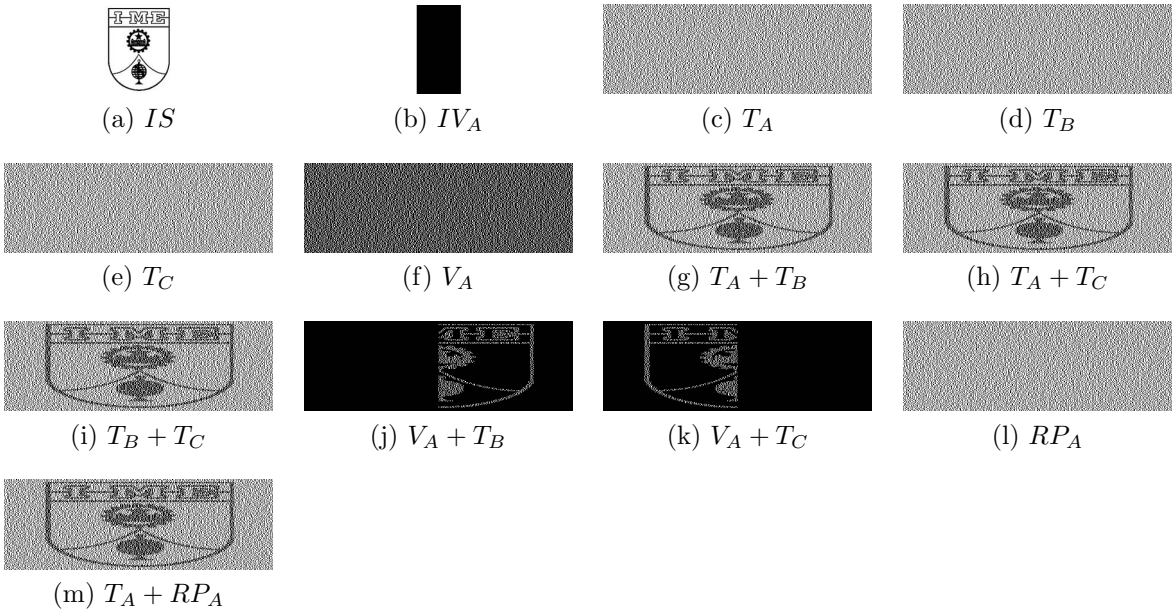
(i) $T_B + T_C$ (j) $V_A + T_B$ (k) $V_A + T_C$ (l) RP_A

(m) $T_A + RP_A$

FIG. 4.5: Demonstração de $T_A + RP_A = IS$ no HCT com IV_A predominantemente preta.

Esta diferença entre as imagens escolhidas por Alice em cada experimento interferiu nos resultados obtidos por ela. No primeiro experimento, realizado com a IV_A predominantemente branca, é possível observar que a IS, representada pelo logo do IME, não pode ser identificada visualmente através da sobreposição $T_A + RP_A$.

No entanto, o segundo experimento, que foi realizado com a IV_A predominantemente preta, revelou o resultado que realmente interessa para Alice. Ele indica a possibilidade de reconstrução da IS individualmente, pois nesse caso o logo do IME pode ser identificado visualmente através da sobreposição $T_A + RP_A$. O terceiro experimento, realizado com a IVA completamente preta, confirmou o sucesso do ataque.



(a) IS (b) IV_A (c) T_A (d) T_B

(e) T_C (f) V_A (g) $T_A + T_B$ (h) $T_A + T_C$

(i) $T_B + T_C$ (j) $V_A + T_B$ (k) $V_A + T_C$ (l) RP_A

(m) $T_A + RP_A$

FIG. 4.6: Demonstração de $T_A + RP_A = IS$ no HCT com IV_A completamente preta.

Portanto, é possível realizar uma análise preliminar sobre os experimentos demonstrados na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6. Para que Alice realize o ataque com sucesso, é necessário que a IV_A escolhida seja predominantemente composta por pixels pretos. Quanto maior for a quantidade de pixels pretos em IV_A, melhor será a identificação visual que Alice poderá realizar sobre a IS, através de $T_A + RP_A$. Uma análise mais detalhada sobre este ataque será apresentada na Seção 4.6.

4.4 PREVENÇÃO HT

O esquema de prevenção HT é um $ABCPS$ desenvolvido por HU e TZENG (2007). A estrutura básica deste esquema é apresentada no fluxograma da FIG. 4.7. Nele, os participantes $P_0, ..., P_{n-1}$ recebem transparências originais $T_0, ..., T_{n-1}$ e transparências extras de verificação $V_0, ..., V_{n-1}$. Cada T_i é construída por uma versão adaptada de um $(k, n)VCS$. A transparência de verificação V_i é utilizada para verificar a integridade de cada transparência T_j, onde $j = 0, ..., n-1$, e $j \neq i$.

Cada participante P_i deve enviar ao esquema, através de canais seguros, uma imagem de verificação IV_i para ser autenticada durante a verificação de integridade das transparências dos outros participantes. A construção de $T_0, ..., T_{n-1}$ é baseada em uma versão adaptada de um $(k, n)VCS$, através da adição de 2 colunas em cada matriz S_0 e S_1, de

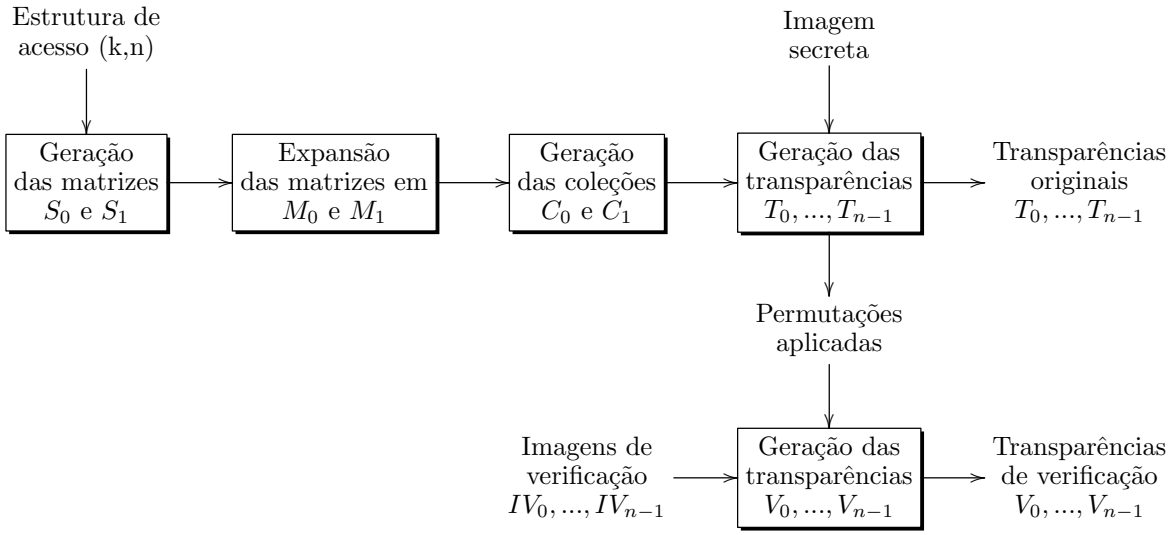


FIG. 4.7: Fluxo para a construção de $T_0, ..., T_{n-1}$ e $V_0, ..., V_{n-1}$ no HT. Adaptação: (CIMATO e YANG, 2011).

forma que cada pixel da imagem secreta seja expandido em $m + 2$ subpixels. A construção de $V_0, ..., V_{n-1}$ é baseada em um $(2, 2)VCS$, realizado entre os pixels das duas colunas concatenadas a S_0 e S_1 de T_i e os pixels correspondentes em V_i.

Para construir $T_0, ..., T_{n-1}$ e $V_0, ..., V_{n-1}$, o esquema de prevenção HT deve gerar as versões expandidas M_0 e M_1 das duas matrizes S_0 e S_1, respectivamente. Cada matriz expandida possui dimensões de $n \times (m + 2)$ elementos, e é composta pela concatenação da matriz correspondente S_0 ou S_1, com duas colunas de bits, da seguinte forma:

$$M_0 = \left[\begin{array}{cc|c} 1 & 0 & \\ \vdots & \vdots & S_0 \\ 1 & 0 & \end{array}\right]; M_1 = \left[\begin{array}{cc|c} 1 & 0 & \\ \vdots & \vdots & S_1 \\ 1 & 0 & \end{array}\right]$$

Cada pixel de IV_i deve ser representado por m_0 ou m_1 na posição correspondente em V_i. As matrizes m_0 e m_1 definem cada bloco $B_p^{V_i}$, possuem dimensões de $1 \times (m + 2)$ elementos e são definidas da seguinte forma:

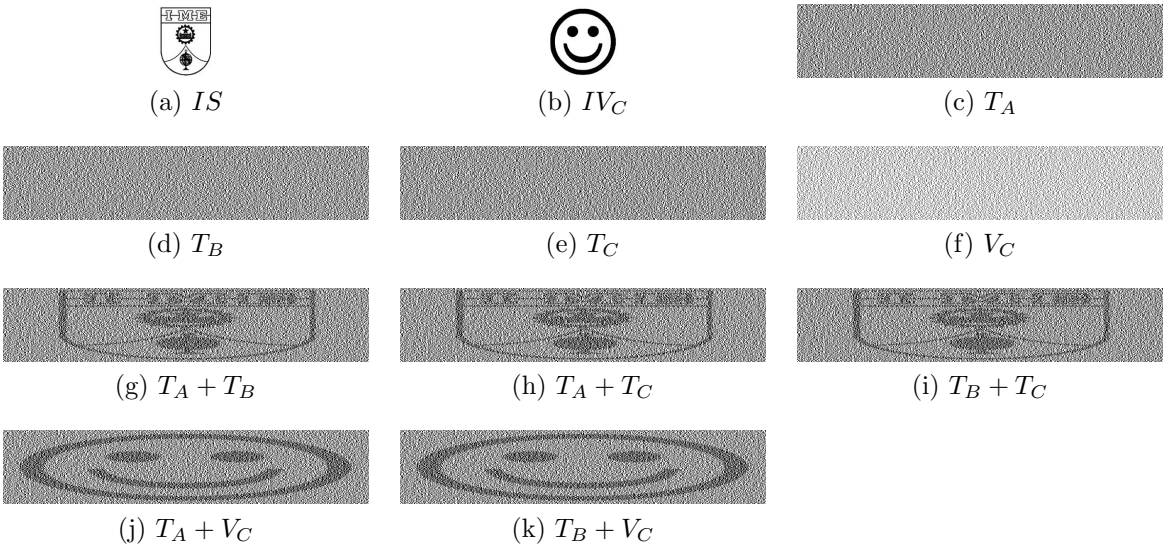
$$m_0 = \left[\begin{array}{ccccc} 1 & 0 & 0 & \dots & 0 \end{array}\right]; m_1 = \left[\begin{array}{ccccc} 0 & 1 & 0 & \dots & 0 \end{array}\right]$$

Portanto, os dois primeiros subpixels de $B_p^{T_0}, ..., B_p^{T_{n-1}}$ e de $B_p^{V_0}, ..., B_p^{V_{n-1}}$ codificam $IV_0, ..., IV_{n-1}$ através de um $(2, 2)VCS$. Caso o p-ésimo pixel da IV_i seja branco, então o

resultado da sobreposição dos subpixels em $B_p^{V_i} + B_p^{T_j}$ forma $[10] + [10] = [10]$. De forma semelhante, caso o p-ésimo pixel da IV_i seja preto, então o resultado da sobreposição dos subpixels em $B_p^{V_i} + B_p^{T_j}$ forma $[01] + [10] = [11]$.

A última etapa consiste na aplicação de uma permutação para cada conjunto de blocos $B_p^{T_0}, ..., B_p^{T_{n-1}}, B_p^{V_0}, ..., B_p^{V_{n-1}}$ correspondentes ao p-ésimo pixel da IS. Como as posições dos subpixels utilizados na autenticação são iguais, HU e TZENG (2007) afirmaram que, caso o participante P_i conheça $T_0, ..., T_{n-1}$, ainda assim ele não será capaz de definir as posições dos subpixels pretos de IV_j, e por isso não será capaz de construir T_i' que passe na verificação $T_i' + V_j$ realizada pelo participante P_j.

Sob o ponto de vista dos participantes Alice, Bob e Carol, as duas principais diferenças entre os esquemas de prevenção HCT e HT estão relacionadas com as dimensões das transparências $T_0, ..., T_{n-1}$ e $V_0, ..., V_{n-1}$, que no HT são maiores, devido à adição dos subpixels de autenticação, e com a reconstrução de IV_i, definida pela sobreposição $V_i + T_j$, que no HCT ocupa somente a região R_{ij}, e no HT ocupa toda a extensão de V_i. O resultado do experimento é apresentado na FIG. 4.8.



(a) IS (b) IV_C (c) T_A

(d) T_B (e) T_C (f) V_C

(g) $T_A + T_B$ (h) $T_A + T_C$ (i) $T_B + T_C$

(j) $T_A + V_C$ (k) $T_B + V_C$

FIG. 4.8: Demonstração de $T_A + V_C = IV_C$ e $T_B + V_C = IV_C$ no HT.

Na FIG. 4.8, a imagem secreta IS pode ser visualizada em (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem de verificação IV_C escolhida por Carol pode ser visualizada em (b). Foi definido um *smile* de cor predominantemente branca com 150×150 pixels, para ser a IV_C.

As três transparências originais T_A, T_B e T_C podem ser visualizadas em (c), (d) e (e), respectivamente. A transparência de verificação de Carol V_C pode ser visualizada em (f). A construção de T_A, T_B e T_C foi realizada a partir de IS com base no $(2,3)VCS$, modificado pelo esquema de prevenção HT, com $m = 5$. Cada T_i possui 150×750 pixels. As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$ podem ser visualizadas em (g), (h) e (i), respectivamente. Cada sobreposição define a reconstrução de IS.

A construção de V_C foi realizada a partir de IV_C. Esta transparência de verificação também possui 150×750 pixels. As sobreposições $T_A + V_C$ e $T_B + V_C$ podem ser visualizadas em (j) e (k), respectivamente. A sobreposição $T_A + V_C$ define a reconstrução de IV_C em toda a área de V_C. Da mesma forma, a sobreposição $T_B + V_C$ define a reconstrução de IV_C em toda a área de V_C.

4.5 ATAQUE AO HT: MAPEAMENTO DOS SUBPIXELS DE AUTENTICAÇÃO ATRAVÉS DE $IV_0, ..., IV_{N-2}$ COMPLEMENTARES

O ataque ao esquema HT foi realizado por LIU, WU e LIN (2011). Sabe-se que cada linha das matrizes M_0 e M_1 são formadas pela concatenação dos subpixels de autenticação com a linha correspondente nas matrizes S_0 e S_1, respectivamente, e que as posições desses dois subpixels são iguais nos blocos $B_p^{T_0}, ..., B_p^{T_{n-1}}$. Então, LIU, WU e LIN (2011) afirmaram que, se os participantes desonestos $P_0, ..., P_{n-2}$ forem capazes de localizar essas posições em $B_p^{T_0}, ..., B_p^{T_{n-2}}$, então eles poderão replicá-los em $B_p^{T'_0}, ..., B_p^{T'_{n-2}}$, para que possam modificar os subpixels restantes, construídos pela matriz S_0 ou S_1, através das transformações definidas no Capítulo 3. A repetição deste procedimento para cada pixel resultaria em transparências $T_0, ..., T_{n-2}$, que passariam pela verificação da vítima P_{n-1}.

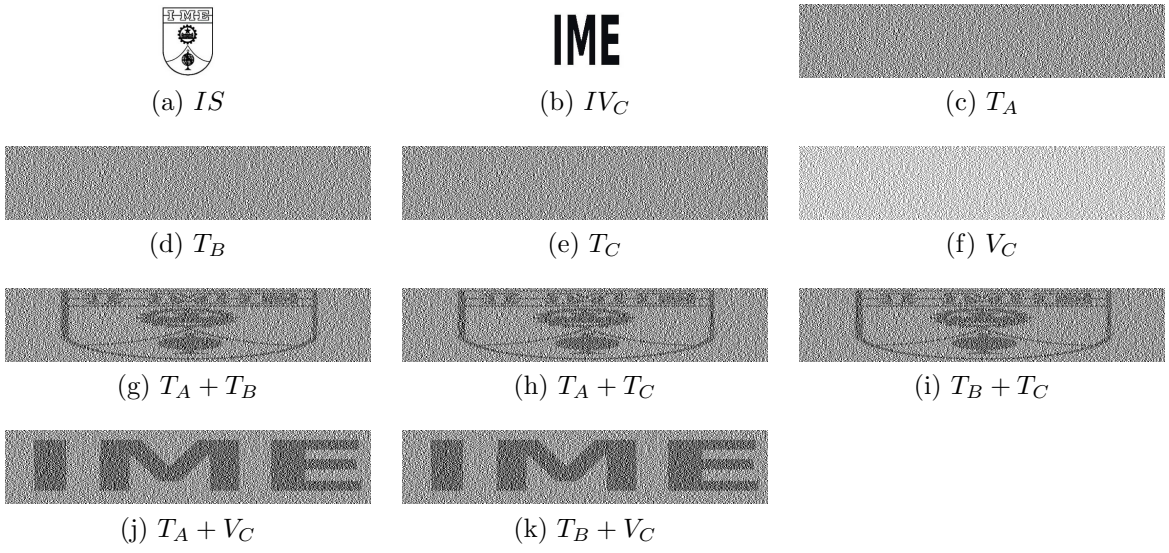
As posições dos dois subpixels de autenticação podem ser mapeadas em $B_p^{T'_0}, ..., B_p^{T'_{n-2}}$, da seguinte forma: sabe-se que em $B_p^{T_i}$ um dos subpixels é preto e o outro é branco, e que esses dois subpixels formam um $(2,2)VCS$ com $B_p^{V_i}$. Em $B_p^{V_i}$ há dois subpixels na mesma posição que os subpixels de autenticação em $B_p^{T_i}$. Um desses subpixels em $B_p^{V_i}$ é preto. O detalhe a ser observado é que este subpixel preto é único em $B_p^{V_i}$, e todos os outros subpixels restantes são brancos.

Portanto, caso o p-ésimo pixel em IV_i seja branco, o subpixel preto em $B_p^{V_i}$ será relacionado ao subpixel preto de autenticação em $B_p^{T_i}$. Caso o p-ésimo pixel em IV_i seja preto, o subpixel preto em $B_p^{V_i}$ será relacionado ao subpixel branco de autenticação em $B_p^{T_i}$. Como o bloco $B_p^{V_i}$ possui um subpixel preto e todos os outros brancos, então

um participante desonesto P_i será capaz de localizar somente a posição do subpixel de autenticação em $B_p^{T_i}$ correspondente subpixel preto de $B_p^{V_i}$.

Os participantes desonestos $P_0, ..., P_{n-2}$ podem obter todas as posições dos subpixels de autenticação pretos e brancos pela escolha combinada de $IV_0, ..., IV_{n-2}$ com cores complementares. Este procedimento permitirá que eles localizem as posições de todos os subpixels de autenticação pretos e brancos em $B_p^{T_0}, ..., B_p^{T_{n-2}}$. O mapeamento resultante deste procedimento realizado para cada pixel da IS, permite que $P_0, ..., P_{n-2}$ construam $T'_0, ..., T'_{n-2}$ através do processo de execução da fraude definido na Capítulo 3.

É possível supor que Alice e Bob combinem a escolha de IV_A e IV_B. Então, eles poderiam localizar as posições dos subpixels de autenticação em $B_p^{T_A}$ e $B_p^{T_B}$, através da análise de $B_p^{V_A}$ e $B_p^{V_B}$. Em seguida, eles replicariam esses subpixels em $B_p^{T'_A}$ e $B_p^{T'_B}$, para que pudessem modificar os subpixels restantes seguindo as transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$, necessárias para a execução da fraude. Ao repetir este procedimento para cada pixel da IS, Alice e Bob poderiam construir T'_A e T'_B, que passariam pela verificação de Carol. O resultado do experimento é apresentado na FIG. 4.9 e na FIG. 4.10.



(a) IS (b) IV_C (c) T_A

(d) T_B (e) T_C (f) V_C

(g) $T_A + T_B$ (h) $T_A + T_C$ (i) $T_B + T_C$

(j) $T_A + V_C$ (k) $T_B + V_C$

FIG. 4.9: Demonstração de $T_A + V_C = IV_C$ e $T_B + V_C = IV_C$ no ataque ao HT.

Na FIG. 4.9, é demonstrada a verificação de Carol durante o ataque ao HT. A imagem secreta IS pode ser visualizada em (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem de verificação IV_C escolhida por Carol pode ser visualizada em (b). Foi definida uma imagem com as letras IME de 150×150 pixels, para ser IV_C.

As três transparências originais T_A, T_B e T_C podem ser visualizadas em (c), (d) e (e), respectivamente. As construções de T_A, T_B e T_C foram realizadas a partir de IS com base no HT. Cada T_i possui 150×750 pixels. A transparência de verificação V_C pode ser visualizada em (f). A construção de V_C foi realizada a partir de IV_C. A transparência de verificação V_C também possui 150×750 pixels.

As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$ podem ser visualizadas em (g), (h) e (i), respectivamente. Cada sobreposição define a reconstrução de IS. As sobreposições $T_A + V_C$ e $T_B + V_C$ podem ser visualizadas em (j) e (k), respectivamente. A sobreposição $T_A + V_C$ define a reconstrução de IV_C em toda a área de V_C. Da mesma forma, a sobreposição $T_B + V_C$ define a reconstrução de IV_C em toda a área de V_C.

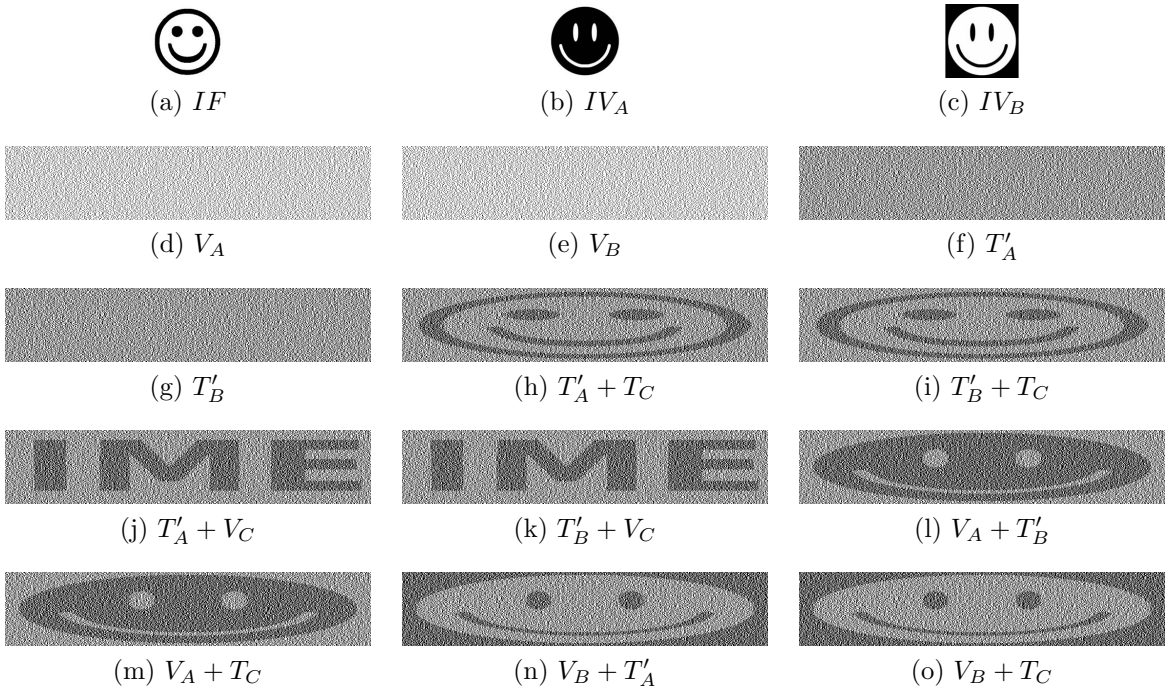


FIG. 4.10: Demonstração de $T'_A + V_C = IV_C$, $T'_B + V_C = IV_C$, $T'_A + T_C = IF$ e $T'_B + T_C = IF$ no ataque ao HT.

Na FIG. 4.10 é demonstrado o sucesso de Alice e Bob no ataque ao HT, ao combinar a escolha de IV_A e IV_B. A imagem falsa IF escolhida por eles pode ser visualizada em (a). Foi definido um *smile* de cor predominantemente branca com 150×150 pixels, para ser a IF. As imagens de verificação IV_A e IV_B escolhidas por Alice e Bob podem ser visualizadas em (b) e (c), respectivamente. Foram definidos dois *smiles* com cores complementares com 150×150 pixels, para ser IV_A e IV_B.

As duas transparências de verificação V_A e V_B podem ser visualizadas em (d) e (e), respectivamente. As construções de V_A e V_B foram realizadas a partir de IV_A e IV_B, respectivamente. As transparências de verificação V_A e V_B também possuem 150×750 pixels. As duas transparências falsas T'_A e T'_B podem ser visualizadas em (f) e (g), respectivamente. A construção de T'_A e T'_B foi realizada a partir de IF com base na construção descrita nesta Seção. Cada transparência falsa T'_A e T'_B também possui 150×750 pixels.

As sobreposições $T'_A + T_C$ e $T'_B + T_C$ podem ser visualizadas em (h) e (i), respectivamente. A sobreposição $T'_A + T_C$ define a reconstrução de IF em toda a área de T_C. Da mesma forma, a sobreposição $T'_B + T_C$ define a reconstrução de IF em toda a área de T_C. As sobreposições $T'_A + V_C$ e $T'_B + V_C$ podem ser visualizadas em (j) e (k), respectivamente. A sobreposição $T'_A + V_C$ define a reconstrução de IV_C em toda a área de V_C. Da mesma forma, a sobreposição $T'_B + V_C$ define reconstrução de IV_C em toda a área de V_C.

As sobreposições $V_A + T'_B$ e $V_A + T_C$ podem ser visualizadas em (l) e (m), respectivamente. A sobreposição $V_A + T'_B$ define a reconstrução de IV_A em toda a área de V_A. Da mesma forma, a sobreposição $V_A + T_C$ define reconstrução de IV_A em toda a área de V_A. Finalmente, as sobreposições $V_B + T'_A$ e $V_B + T_C$ podem ser visualizadas em (n) e (o), respectivamente. A sobreposição $V_B + T'_A$ define a reconstrução de IV_B em toda a área de V_B. Da mesma forma, a sobreposição $V_B + T_C$ define reconstrução de IV_B em toda a área de V_B.

4.6 ANÁLISE SOBRE OS ATAQUES AOS ESQUEMAS HCT E HT

A verificação da integridade fornecida pelo esquema de prevenção HCT funcionou corretamente. A fraude demonstrada no experimento da FIG. 3.3 poderia ser detectada. O experimento demonstrado na FIG. 4.2 confirmou que Carol tornou-se capaz de verificar, através da prevenção HCT, a integridade de T_A ou T_B, caso ela suspeite que essas transparências não são originais ou que a imagem reconstruída após uma das sobreposições $T_A + T_C$ ou $T_B + T_C$ não representa a imagem secreta IS. No entanto, HU e TZENG (2007) e LIU, WU e LIN (2011) identificaram vulnerabilidades no esquema HCT.

O primeiro ataque ao esquema de prevenção HCT, realizado por HU e TZENG (2007), foi demonstrado na FIG. 4.3. Neste experimento, Alice construiu T'_A de forma que cada $B_p^{T_A}$ correspondente a R_{CA} não fosse alterado. O resultado foi a reconstrução de IV_A após a verificação realizada por Carol, através da sobreposição $T'_A + V_C$. Ainda neste experimento, Bob construiu T'_B de forma que cada $B_p^{T_B}$ correspondente a R_{CB} não fosse alterado. O

resultado foi a reconstrução de IV_B após a verificação realizada por Carol, através da sobreposição $T'_B + V_C$. O sucesso de Alice e Bob neste ataque, requer o conhecimento das regiões R_{CA} e R_{CB}, que verificam a integridade de T_A e T_B, respectivamente.

Esta vulnerabilidade explorada por HU e TZENG (2007) poderia ser solucionada se Carol fosse capaz de verificar a integridade de toda a extensão de T_A, T_B, T'_A e T'_B. Embora a solução para esta vulnerabilidade seja clara, há diversas formas de implementá-la. Uma delas foi desenvolvida por HU e TZENG (2007), mas também possui vulnerabilidades.

A implementação da correção sugerida neste trabalho requer que as dimensões de V_i sejam maiores que as de T_i, e que seja utilizado algum mecanismo de deslocamento das transparências durante as verificações, devido à diferença de dimensões entre T_i e V_i. Mais especificamente, deve ser desenvolvida uma versão adaptada do esquema de SHYU et al. (2007), cuja definição foi apresentada na Seção 2.5, como mecanismo de construção da transparência circular que forneceria para Carol a capacidade de verificar a integridade de T_A, T_B, T'_A e T'_B, através de sobreposições obtidas com algumas rotações de V_C.

O segundo ataque ao esquema de prevenção HCT, realizado por LIU, WU e LIN (2011) foi demonstrado na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6. Este ataque presume que Alice seja capaz de reconstruir as partes de T_B e T_C, correspondentes a R_{AB} e R_{AC}, respectivamente, a partir de V_A e IV_A. Para que este ataque seja realizado com sucesso, é necessário que Alice escolha IV_A predominantemente composta por pixels pretos. Quanto maior for a quantidade de pixels pretos em IV_A, melhor será a identificação visual sobre a reconstrução da IS, realizada através da sobreposição $T_A + RP_A$.

Há uma relação entre esta vulnerabilidade e o processo de construção da V_A no HCT. A cor resultante das sobreposições entre $B_p^{V_A} + B_p^{T_B}$ ou $B_p^{V_A} + B_p^{T_C}$ é definida pelo posicionamento do subpixel preto em $B_p^{T_B}$ ou $B_p^{T_C}$, respectivamente, pois a construção de $B_p^{V_A}$ identifica o único subpixel preto em $B_p^{T_B}$ na região R_{AB} ou $B_p^{T_C}$ na região R_{AC}, quando o p-ésimo pixel em IV_A for preto. No entanto, a construção de $B_p^{V_A}$ identifica aleatoriamente um dos subpixels brancos $B_p^{T_B}$ na região R_{AB} ou $B_p^{T_C}$ na região R_{AC}, quando o p-ésimo pixel em IV_A for branco. Esta aleatoriedade gera incerteza no ataque realizado por Alice.

Portanto, quanto maior for o número de pixels pretos em IV_A, maior será a quantidade de blocos reconstruídos corretamente em R_A, e maior também será a possibilidade de sucesso na identificação visual da IS, realizada por Alice, após a reconstrução obtida pela sobreposição $T_A + RP_A$. O caso perfeito para Alice seria a escolha de uma imagem de verificação IV_A formada completamente por pixels pretos, conforme o experimento

demonstrado na FIG. 4.6. Neste caso, a reconstrução das regiões R_{AB} e R_{AC} em R_A é perfeita e a IS é completamente reconstruída pela sobreposição $T_A + RP_A$.

Esta vulnerabilidade explorada por LIU, WU e LIN (2011) poderia ser corrigida pela inclusão no esquema de um módulo capaz de validar IV_A, IV_B e IV_C, através da limitação da quantidade de pixels pretos contidos em cada imagem de verificação. Adicionalmente, o módulo deve ser capaz de inverter as cores de todos os pixeis de qualquer imagem de verificação que possua a quantidade de pixels pretos superior ao limite estabelecido. Esta função tornaria dispensável a rejeição das imagens reprovadas na validação. Mais detalhes sobre a construção do módulo de validação serão apresentados no Capítulo 5.

A verificação da integridade fornecida pelo esquema de prevenção HT funcionou corretamente. Neste caso, a fraude demonstrada no experimento da FIG. 3.3 não pode ser realizada. Além disso, o esquema de prevenção HT é seguro contra os ataques realizados contra o esquema HCT, demonstrados na FIG. 4.3, na FIG. 4.4, na FIG. 4.5 e na FIG. 4.6, pois cada verificação $V_C + T_A$ e $V_C + T_B$ ocupa toda a área de V_C, e o processo de construção de V_C é baseado em um $(2, 2)VCS$ independente da construção de T_C, através da adição de subpixels relacionados com a autenticação das imagens de verificação. No entanto, uma vulnerabilidade no HT foi identificada por LIU, WU e LIN (2011).

O ataque ao esquema de prevenção HT, realizado por LIU, WU e LIN (2011), foi demonstrado na FIG. 4.9 e na FIG. 4.10. Nesse experimento, Alice e Bob combinaram a escolha de IV_A e IV_B e se tornaram capazes de localizar as posições dos subpixels de autenticação em $B_p^{T_A}$ e $B_p^{T_B}$, através da análise de $B_p^{V_A}$ e $B_p^{V_B}$. Após repetir este procedimento para cada pixel da IS, eles construíram T'_A e T'_B, realizando as transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ sobre os subpixels restantes. Desta forma, T'_A e T'_B passaram na verificação de Carol, realizada pelas sobreposições $V_C + T'_A$ e $V_C + T'_B$.

Esta vulnerabilidade explorada por LIU, WU e LIN (2011) indica a qualquer projeto de um novo esquema de prevenção contra fraude que a utilização de subpixels especificamente na autenticação das imagens de verificação tornará o esquema vulnerável à fraude demonstrada na FIG. 3.3, se Alice e Bob conseguirem localizar as posições dos subpixels de autenticação em $B_p^{T_A}$ e $B_p^{T_B}$. A correção sobre a vulnerabilidade do HT sugerida neste trabalho é a utilização de subpixels extras, com a definição aleatória dos subpixels de autenticação em um bloco, além de um mecanismo de permutação baseado em múltiplas imagens de verificação, que invalidaria qualquer combinação entre Alice e Bob, por tornar indeterminado o conhecimento que possuem sobre as transparências de Carol.

A análise sobre os ataques às vulnerabilidades dos esquemas HCT e HT apresentada nesta Seção fornece a base do projeto para o desenvolvimento de um novo esquema de prevenção contra fraude em Criptografia Visual, conforme ilustrado na FIG. 4.11.

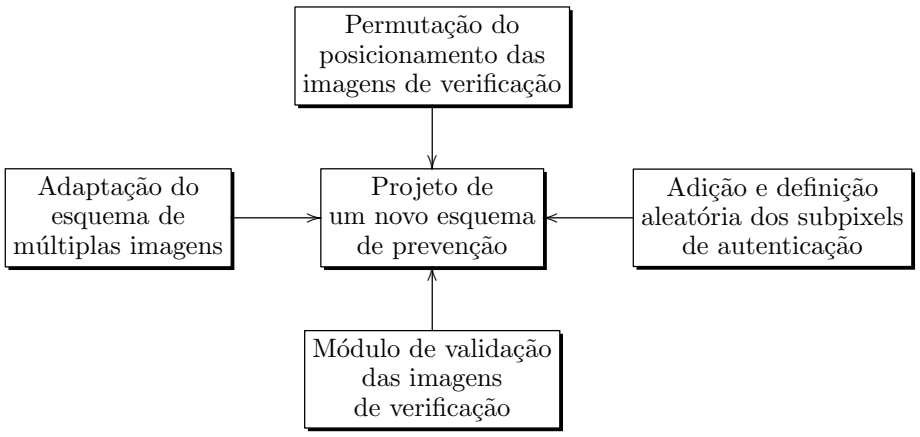


FIG. 4.11: Base para o projeto de um novo esquema de prevenção contra fraude.

A adaptação do esquema que codifica múltiplas imagens, desenvolvido por SHYU et al. (2007) forneceria a segurança diante do ataque definido por HU e TZENG (2007) contra o HCT, através da capacidade de verificação da integridade de toda a extensão das transparências dos outros participantes, com base na utilização de transparências circulares. A adição de um módulo de validação ao projeto forneceria a segurança contra o ataque definido por LIU, WU e LIN (2011) ao HCT, através da capacidade de limitar a quantidade de pixels pretos nas imagens de verificação informadas pelos participantes. Um mecanismo de permutação do posicionamento das imagens que devem ser autenticadas durante o processo de verificação das transparências forneceria a segurança contra o ataque definido por LIU, WU e LIN (2011) contra o esquema de prevenção HT, pois ele inviabiliza a combinação de imagens complementares, e aumenta a incerteza relacionada com as informações que os participantes desonestos possuem sobre a vítima. Finalmente, o aumento da expansão dos pixels poderia incorporar informações adicionais, e seriam definidos aleatoriamente para a autenticação ou construção dos blocos, fornecendo também a segurança diante do ataque definido por LIU, WU e LIN (2011) contra o esquema HT.

5 CONSTRUÇÃO DA NOVA PREVENÇÃO CONTRA FRAUDE

O objetivo deste Capítulo é apresentar o esquema de prevenção contra fraude desenvolvido neste trabalho, através de uma exposição detalhada dos conceitos e experimentos relacionados com os métodos de construção das transparências originais e circulares de verificação, que devem ser entregues aos participantes, além de detalhar o processo de validação das imagens de verificação que devem ser informadas pelos participantes ao esquema e posteriormente autenticadas por eles durante a verificação da integridade das transparências deles. Este Capítulo está organizado da seguinte forma. Na Seção 5.1, será apresentada uma visão geral da estrutura do novo esquema de prevenção contra fraude. Na Seção 5.2, as definições formais sobre a construção das transparências originais dos participantes serão apresentadas. Nesta Seção também será apresentado um experimento que demonstra construção das transparências originais em um $(2, 3)VCS$. Na Seção 5.3, as definições formais sobre a construção das transparências circulares de verificação dos participantes serão apresentadas. Nesta Seção também será apresentado um experimento que simula a escolha das imagens de verificação e demonstra a construção das transparências circulares de verificação em um $(2, 3)VCS$. Na Seção 5.4, será apresentado o resultado de um experimento que demonstra o processo de verificação realizado por Carol através das sobreposições com rotações entre a sua transparência circular de verificação e as transparências originais de Alice e Bob. Na Seção 5.5, o módulo de validação das imagens de verificação será apresentado. O Capítulo será concluído na Seção 5.6 com uma breve análise sobre a necessidade de suporte aos aspectos de segurança do novo esquema.

5.1 DEFINIÇÕES BÁSICAS SOBRE O NOVO ESQUEMA

O esquema de prevenção contra fraude desenvolvido neste trabalho é um $ABCPS$, cuja estrutura básica é apresentada no fluxograma da FIG. 5.1. Neste esquema, os participantes $P_0, ..., P_{n-1}$ recebem as transparências originais $T_0, ..., T_{n-1}$ e as transparências circulares extras de verificação $V_0, ..., V_{n-1}$. Cada T_i é construída por uma versão adaptada de um $(2, n)VCS$, através da adição de m subpixels em cada matriz S_0 e S_1, de forma que cada pixel da imagem original seja expandido em $2m$ subpixels. Cada V_i é utilizada para verificar a integridade de cada transparência T_j, onde $j = 0, 1, ..., n - 1$, e $j \neq i$.

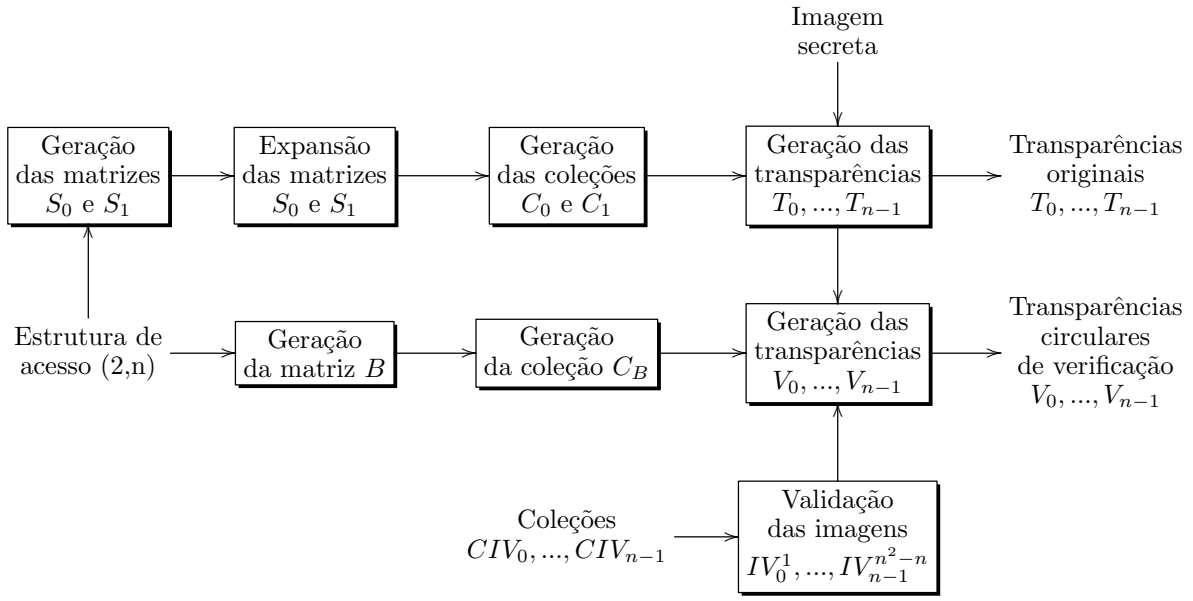


FIG. 5.1: Fluxo para a construção de $T_0, ..., T_{n-1}$ e $V_0, ..., V_{n-1}$ no novo esquema.

Cada participante P_i deve enviar ao esquema, através de canais seguros, uma coleção CIV_i de $n^2 - n$ imagens de verificação para serem autenticadas durante a verificação da integridade das transparências dos outros participantes. É necessário que cada imagem de verificação IV_i^z, onde $1 \leq z \leq n^2 - n$, possua alguns pré-requisitos relacionados com a segurança do esquema e por isso deve ser submetida a um processo de validação. Cada V_i é dividida em $n^3 - n^2$ regiões R_{xy}, onde $0 \leq x < n^2 - n$ e $0 \leq y < n$. A sobreposição $V_i + T_j$ reconstrói em cada R_{xy}, uma imagem de verificação IV_i^z.

Desta forma, os famosos personagens Alice, Bob e Carol possuem além das transparências originais T_A, T_B e T_C, as transparências circulares de verificação V_A, V_B e V_C, respectivamente. Neste esquema, Carol é capaz de verificar a integridade de T_A e T_B através de V_C. Assim como foi definido por HORNG, CHEN e TSAI (2006), o processo é composto pelas fases de inicialização, autenticação e decodificação.

Na inicialização, os participantes escolhem individualmente suas coleções CIV_A, CIV_B e CIV_C, e as enviam com segurança ao esquema. Na fase de autenticação, Carol deve posicionar uma das transparências T_A ou T_B em sua transparência de verificação V_C, e rotacionar $n^2 - n$ vezes T_A ou T_B sobre V_C, nos ângulos $\frac{360^o}{z}$, onde $1 \leq z \leq n^2 - n = 6$.

Durante a fase de autenticação, cada imagem de verificação IV_C^z deve ser completamente reconstruída. Se a autenticação for efetuada com sucesso, Carol pode sobrepor T_C com T_A ou T_B e concluir a fase de decodificação. Caso contrário, Carol deve rejeitar a transparência de Alice ou de Bob.

5.2 CONSTRUÇÃO DAS TRANSPARÊNCIAS ORIGINAIS $T_0, ..., T_{N-1}$

A geração das matrizes S_0 e S_1 segue os padrões definidos no $(2, n)VCS$. Conforme foi descrito na Seção 3.1, as duas matrizes S_0 e S_1 possuem dimensões $n \times m$, onde $m = n$, e são construídas de forma que a matriz S_0 possua o valor 1 em todas as posições da primeira coluna com o valor 0 nas posições referentes às outras colunas, e a matriz S_1 possua o valor 1 em todas as posições de sua diagonal principal com o valor 0 nas posições restantes. Portanto, as matrizes S_0 e S_1 podem ser definidas da seguinte forma:

$$S_0 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}; S_1 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

O processo de expansão das matrizes S_0 e S_1 deve gerar as versões modificadas M_0 e M_1 com dimensões $n \times (2m)$. A estrutura de cada matriz M_0 ou M_1 é resultante da concatenação entre a matriz correspondente S_0 ou S_1 em um $(2, n)VCS$ com uma cópia da matriz S_1. A cópia de S_1 concatenada à matriz S_0 será identificada como S_1', e a cópia de S_1 concatenada à matriz S_1 será identificada como S_1''. O esquema define, através de uma escolha aleatória, o posicionamento das matrizes S_1' e S_1'' no processo de concatenação.

$$M_0 = \left[\begin{array}{c|c} S_0 & S_1' \end{array}\right] ou \left[\begin{array}{c|c} S_1' & S_0 \end{array}\right];$$

$$M_1 = \left[\begin{array}{c|c} S_1 & S_1'' \end{array}\right] ou \left[\begin{array}{c|c} S_1'' & S_1 \end{array}\right];$$

Desta forma, é possível definir que o processo de expansão das matrizes S_0 e S_1 deverá resultar nas duas matrizes M_0 e M_1 com os seguintes valores:

$$M_0 = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{array}\right] ou \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 1 & 0 & \cdots & 0 \end{array}\right];$$

$$M_1 = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 1 \end{array}\right]$$

A coleção C_0 é formada por todas as combinações possíveis entre os dois conjuntos C_0^0 e C_0^1. O conjunto C_0^0 é composto por todas as matrizes obtidas pelas permutações das colunas da primeira matriz de M_0, que pode ser S_0 ou S_1'. O conjunto C_0^1 é composto por todas as matrizes obtidas pelas permutações das colunas da segunda matriz de M_0, que pode ser S_1' ou S_0. A combinação entre todos os elementos possíveis dos conjuntos C_0^0 e C_0^1 compõem a coleção C_0.

De forma semelhante, a coleção C_1 é formada por todas as combinações possíveis entre os dois conjuntos C_1^0 e C_1^1. O conjunto C_1^0 é composto por todas as matrizes obtidas pelas permutações das colunas da primeira matriz de M_1, que pode ser S_1 ou S_1''. O conjunto C_1^1 é composto por todas as matrizes obtidas pelas permutações das colunas da segunda matriz de M_1, que pode ser S_1'' ou S_1. A combinação entre todos os elementos possíveis dos conjuntos C_1^0 e C_1^1 compõem a coleção C_1.

$$C_0 = \left[\begin{array}{c|c} C_0^0(S_0) & C_0^1(S_1') \end{array}\right] ou \left[\begin{array}{c|c} C_0^0(S_1') & C_0^1(S_0) \end{array}\right];$$

$$C_1 = \left[\begin{array}{c|c} C_1^0(S_1) & C_1^1(S_1'') \end{array}\right] ou \left[\begin{array}{c|c} C_1^0(S_1'') & C_1^1(S_1) \end{array}\right];$$

O esquema utiliza as coleções de matrizes C_0 e C_1 e a imagem secreta IS para gerar as transparências originais $T_0, ..., T_{n-1}$. O p-ésimo pixel da IS será representado pelos blocos $B_p^{T_0}, ..., B_p^{T_{n-1}}$. Os subpixels de cada $B_p^{T_i}$ são definidos por uma matriz de dimensões $2 \times m$. Para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel da imagem secreta IS for branco, o esquema escolhe aleatoriamente uma das matrizes em C_0, e para construir $B_p^{T_0}, ..., B_p^{T_{n-1}}$ quando o p-ésimo pixel da imagem secreta IS for preto, o esquema escolhe aleatoriamente uma das matrizes em C_1.

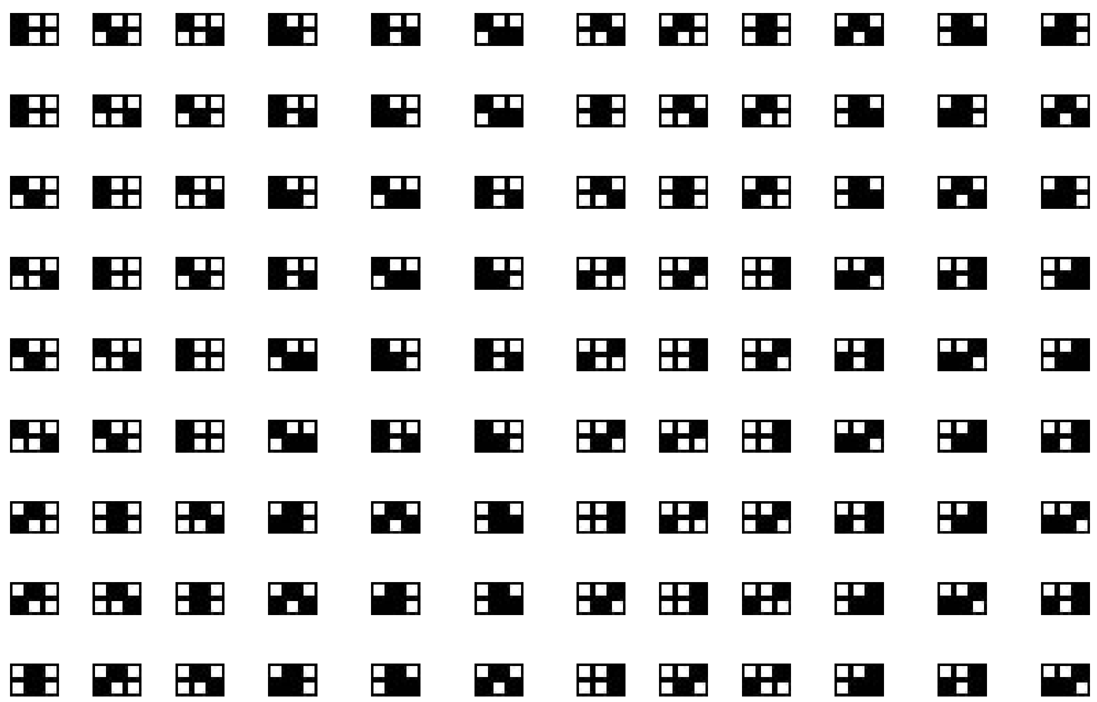
A construção de $B_p^{T_i}$ deve ser obtida pela transformação da matriz i, que representa a i-ésima linha da matriz escolhida e possui dimensões de $1 \times 2m$, na matriz correspondente com dimensões de $2 \times m$. Esta transformação deve ser realizada através do posicionamento da primeira metade da matriz i sobre a segunda. É possível verificar o processo de transformação no exemplo abaixo.

$$i = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{array}\right] \rightarrow \left[\begin{array}{cccc} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{array}\right]$$

Esta transformação deve ser realizada sobre cada linha i, onde $0 \leq i \leq n-1$, da matriz escolhida para o p-ésimo pixel da IS, até que a construção de cada bloco $B_p^{T_i}$ seja concluída. No caso de Alice, Bob e Carol, este processo será repetido na construção de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$, para cada pixel da imagem secreta IS. Caso o p-ésimo pixel da IS seja branco, a construção segue a TAB. 5.1 e a TAB. 5.2. Caso contrário, se o p-ésimo pixel da IS for preto, a construção segue a TAB. 5.3 e a TAB. 5.4.

TAB. 5.1: Construções de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ no novo esquema de prevenção, caso o p-ésimo pixel da IS seja branco.

$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$



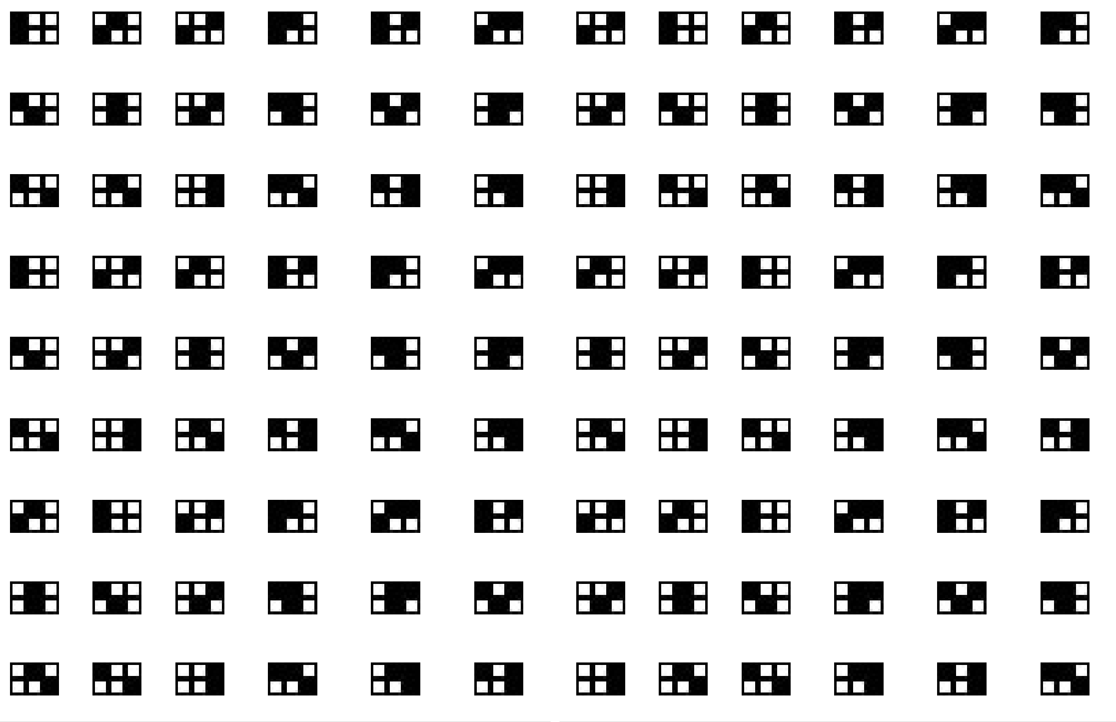
Na TAB. 5.1, são definidas as 18 codificações possíveis de um pixel branco com referência à coleção C_0, formada por todas as combinações possíveis entre os dois conjuntos de matrizes C_0^0 e C_0^1, quando o conjunto C_0^0 for composto por todas as matrizes obtidas pelas permutações das colunas da primeira matriz de M_0, onde $M_0 = S_0$, e o conjunto C_0^1 for composto por todas as matrizes obtidas pelas permutações das colunas da segunda matriz de M_0, onde $M_0 = S_1'$.

$$M_0 = \left[\begin{array}{c|c} S_0 & S_1' \end{array}\right] \rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$C_0 = \left[\begin{array}{c|c} C_0^0(S_0) & C_0^1(S_1') \end{array}\right]$$

TAB. 5.2: Construções de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ no novo esquema de prevenção, caso o p-ésimo pixel da IS seja branco. (Continuação da TAB. 5.1)

$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$



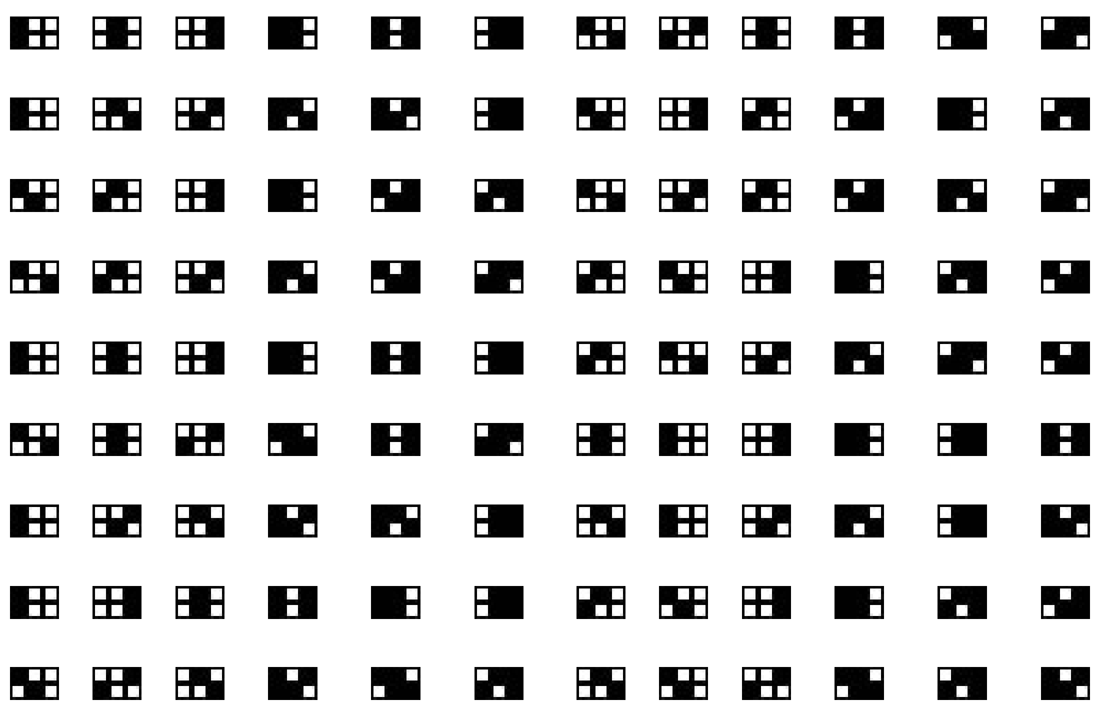
Na TAB. 5.2, são definidas as 18 codificações possíveis de um pixel branco com referência à coleção C_0, formada por todas as combinações possíveis entre os dois conjuntos de matrizes C_0^0 e C_0^1, quando o conjunto C_0^0 for composto por todas as matrizes obtidas pelas permutações das colunas da primeira matriz de M_0, onde $M_0 = S_1'$, e o conjunto C_0^1 for composto por todas as matrizes obtidas pelas permutações das colunas da segunda matriz de M_0, onde $M_0 = S_0$.

$$M_0 = \left[\begin{array}{c|c} S_1' & S_0 \end{array}\right] \rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

$$C_0 = \left[\begin{array}{c|c} C_0^0(S_1') & C_0^1(S_0) \end{array}\right]$$

TAB. 5.3: Construções de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ no novo esquema de prevenção, caso o p-ésimo pixel da IS seja preto.

$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$



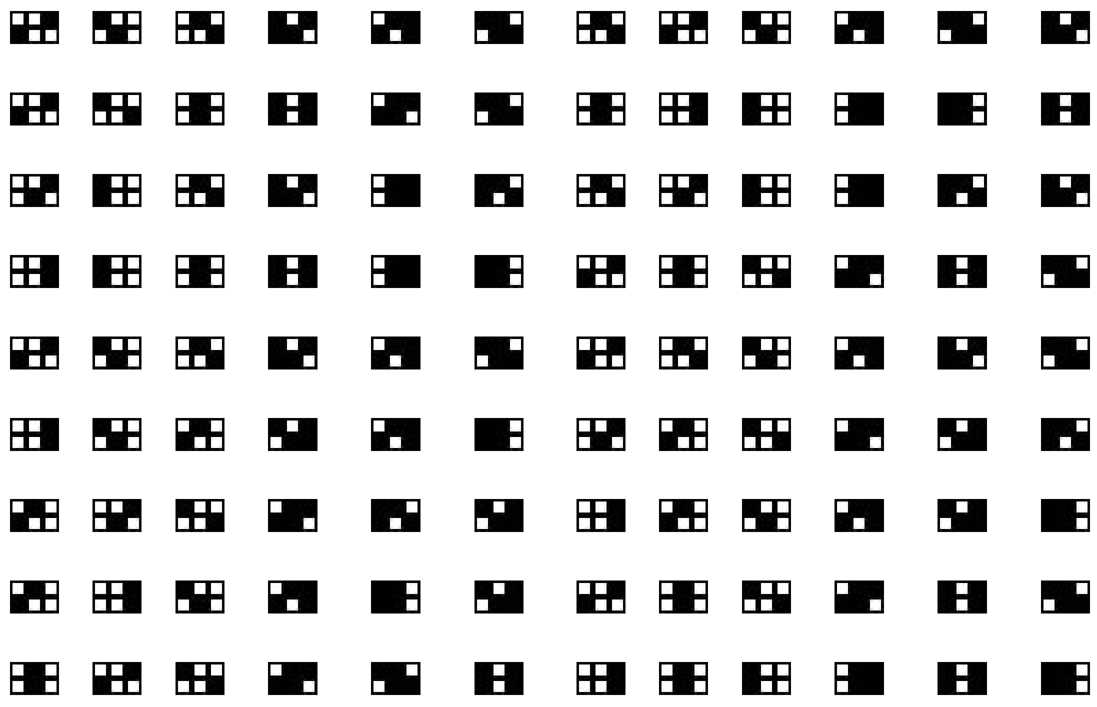
Na TAB. 5.3, são definidas as primeiras 18 de 36 codificações possíveis de um pixel preto com referência à coleção C_1, formada por todas as combinações possíveis entre os dois conjuntos de matrizes C_1^0 e C_1^1. A TAB. 5.4 contém as 18 codificações restantes. Nos dois casos, não importa a ordem das matrizes em M_1, pois $S_1 = S_1''$.

$$M_1 = \left[\begin{array}{c|c} S_1 & S_1'' \end{array}\right] ou \left[\begin{array}{c|c} S_1'' & S_1 \end{array}\right] \rightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

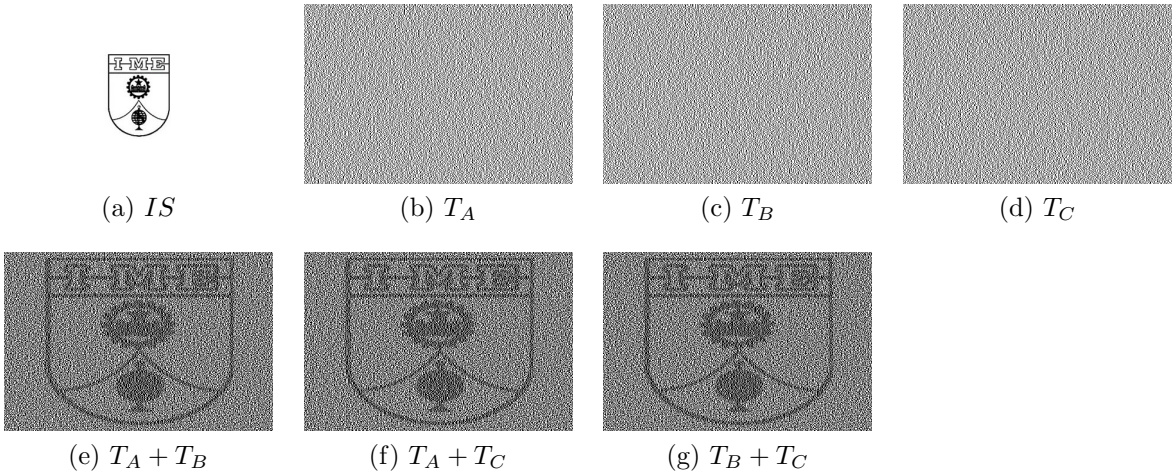
$$C_1 = \left[\begin{array}{c|c} C_1^0(S_1) & C_1^1(S_1'') \end{array}\right] ou \left[\begin{array}{c|c} C_1^0(S_1'') & C_1^1(S_1) \end{array}\right]$$

TAB. 5.4: Construções de $B_p^{T_A}$, $B_p^{T_B}$ e $B_p^{T_C}$ no novo esquema de prevenção, caso o p-ésimo pixel da IS seja preto. (Continuação da TAB. 5.3)

$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$	$B_p^{T_A}$	$B_p^{T_B}$	$B_p^{T_C}$	$B_p^{T_A}+B_p^{T_B}$	$B_p^{T_A}+B_p^{T_C}$	$B_p^{T_B}+B_p^{T_C}$



O resultado do experimento que demonstra a construção das tranparências originais T_A, T_B e T_C, com base no esquema descrito nesta Seção é apresentado na FIG. 5.2.



(a) IS (b) T_A (c) T_B (d) T_C

(e) $T_A + T_B$ (f) $T_A + T_C$ (g) $T_B + T_C$

FIG. 5.2: Demonstração de $T_A + T_B = IS$, $T_A + T_C = IS$ e $T_B + T_C = IS$ no novo esquema de prevenção.

Na FIG. 5.2, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. As três transparências originais T_A, T_B e T_C, que podem ser visualizadas nos itens (b), (c) e (d), respectivamente, foram construídas a partir da IS com base no novo esquema de prevenção contra a fraude apresentado nesta Seção. Cada T_i possui 300×450 pixels. As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (e), (f) e (g), respectivamente, reconstroem a IS.

5.3 CONSTRUÇÃO DAS TRANSPARÊNCIAS DE VERIFICAÇÃO $V_0, ..., V_{N-1}$

As matrizes B_0 e B_1 compõem a base da construção das transparências circulares de verificação $V_0, ..., V_{n-1}$ e possuem dimensões de $n \times m$ elementos, onde $m = n$. Elas são construídas de forma que B_0 possua o valor 0 em todas as posições de sua diagonal principal com o valor 1 nas outras posições, e B_1 possua o valor 1 em todas as posições.

$$B_0 = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}; B_1 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

Em seguida, duas matrizes N_0 e N_1 com dimensões de $n \times 2m$ elementos devem ser construídas com base a partir de B_0 e B_1. A estrutura de N_0 e N_1 é resultante da concatenação entre B_0 e B_1. A diferença entre N_0 e N_1 é o posicionamento de B_0 e B_1.

$$N_0 = \left[\begin{array}{c|c} B_0 & B_1 \end{array}\right]; N_1 = \left[\begin{array}{c|c} B_1 & B_0 \end{array}\right]$$

Desta forma, é possível definir que após o processo de geração das matrizes N_0 e N_1, elas deverão possuir os seguintes valores:

$$N_0 = \left[\begin{array}{ccc|ccc} 0 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 & 1 & \cdots & 1 \end{array}\right]; N_1 = \left[\begin{array}{ccc|ccc} 1 & 1 & \cdots & 1 & 0 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 & 1 & \cdots & 0 \end{array}\right]$$

A matriz N pode ser obtida a partir da concatenação entre N_0 e N_1, através do posicionamento de N_0 sobre N_1, conforme apresentado abaixo:

$$N = \left[\begin{array}{c} N_0 \\ \hline N_1 \end{array}\right];$$

Os valores da matriz N, que possui dimensões de $2n \times 2m$ elementos, podem ser definidos, conforme apresentado a seguir:

$$N = \left[\begin{array}{cccc} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{array}\right];$$

O esquema deve utilizar a matriz N, as transparências $T_0, ..., T_{n-1}$ e as coleções de imagens de verificação $CIV_0, ..., CIV_{n-1}$, para gerar as transparências circulares de verificação $V_0, ..., V_{n-1}$. Cada V_i é dividida em $n^3 - n^2$ regiões R_{xy}, onde $0 \leq x < n^2 - n$ e $0 \leq y < n$. A sobreposição $V_i + T_j$ revela em algum R_{xy}, uma IV_i^z, onde $1 \leq z \leq n^2 - n$.

O processo de construção das transparências circulares de verificação $V_0, ..., V_{n-1}$ deve criar as matrizes $I_0, ..., I_{n-1}$, com dimensões de $n \times n^2 - n$ elementos, que armazenam

referências ordenadas das imagens de verificação $IV_i^1, ..., IV_i^{n^2-n}$ contidas na coleção CIV_i em cada uma das n linhas da matriz I_i.

$$I_i = \begin{bmatrix} IV_i^1 & IV_i^2 & \cdots & IV_i^{n^2-n} \\ IV_i^1 & IV_i^2 & \cdots & IV_i^{n^2-n} \\ \vdots & \vdots & \vdots & \vdots \\ IV_i^1 & IV_i^2 & \cdots & IV_i^{n^2-n} \end{bmatrix}$$

Sobre as linhas da matriz I_i devem ser aplicadas diferentes permutações, de forma que cada uma das n linhas da matriz I_i possua uma combinação diferente de imagens da coleção CIV_i. Em seguida, todas as imagens da matriz I_i devem ser concatenadas, formando uma única imagem temporária, definida como I_i^{tmp}.

O próximo passo no processo de geração da transparência circular de verificação V_i é baseado em cada transparência T_j, onde $j = 0, ..., n-1$, e $j \neq i$. Uma transparência temporária, definida como T_i^{tmp}, é formada pela concatenação de cada T_j. Desta forma, para cada p-ésimo pixel da I_i^{tmp} deve haver um bloco correspondente $B_p^{T_i^{tmp}}$.

Cada $B_p^{V_i}$ é construído com base no p-ésimo pixel de I_i^{tmp} e no bloco $B_p^{T_i^{tmp}}$. Caso o p-ésimo pixel em I_i^{tmp} seja branco, então o esquema deverá escolher aleatoriamente em $B_p^{T_i^{tmp}}$ um dos $n^2 - n - 2$ subpixels brancos para a autenticação. Em seguida, o esquema escolhe na matriz N a linha que, após a transformação em $B_p^{V_i}$, definirá o subpixel branco na posição correspondente. Um exemplo será apresentado a seguir. Seja a, a matriz relacionada ao bloco $B_p^{T_i^{tmp}}$. Se o subpixel branco escolhido aleatoriamente for o marcado em a_x, então a matriz resultante da transformação em $B_p^{V_i}$ após a escolha da linha b em N será representada pela matriz b_x.

$$a = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{bmatrix} \rightarrow a_x = \begin{bmatrix} 1 & X & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$b = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{array}\right] \rightarrow b_x = \begin{bmatrix} 1 & 0 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

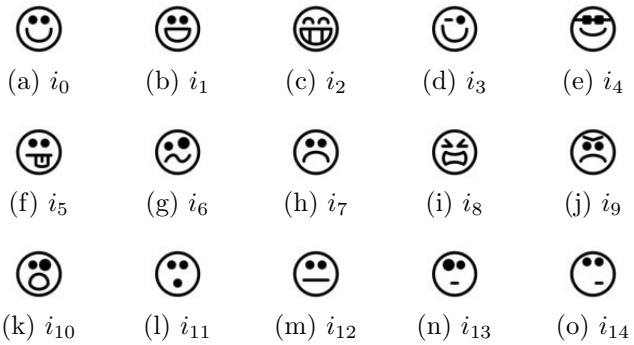
De forma semelhante, caso o p-ésimo pixel em I_i^{tmp} seja preto, então o esquema deverá escolher aleatoriamente em $B_p^{T_i^{tmp}}$ um dos 2 subpixels pretos para a autenticação. Em seguida, o esquema escolhe na matriz N a linha que, após a transformação em $B_p^{V_i}$, definirá

o subpixel preto na posição correspondente. Um exemplo será apresentado a seguir. Seja a, a matriz relacionada ao bloco $B_p^{T_i^{tmp}}$. Se o subpixel preto escolhido aleatoriamente for o marcado em a_x, então a matriz resultante da transformação em $B_p^{V_i}$ após a escolha da linha b em N será representada pela matriz b_x.

$$a = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \end{bmatrix} \rightarrow a_x = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & X & \cdots & 0 \end{bmatrix}$$

$$b = \left[\begin{array}{cccc|cccc} 1 & 1 & \cdots & 1 & 1 & 0 & \cdots & 1 \end{array}\right] \rightarrow b_x = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \end{bmatrix}$$

Esta construção deve ser realizada sobre cada p-ésimo pixel de I_i^{tmp}, até que a construção de cada $B_p^{V_i}$ seja concluída. No caso de Carol, a repetição deste processo para cada $B_p^{V_C}$ resultará em V_C, a transparência circular que será utilizada na verificação da integridade de T_A e T_B. Na fase de inicialização, ela escolhe a sua coleção CIV_C, que deverá conter as $n^2 - n = 3^2 - 3 = 6$ imagens de verificação $IV_C^1, ..., IV_C^6$, que serão autenticadas por Carol durante a verificação da integridade de T_A e T_B. A FIG. 5.3 contém um pequeno grupo de imagens com 50×50 pixels que serão utilizados nos próximos experimentos como imagens de verificação disponíveis para a escolha de Carol.



(a) i_0 (b) i_1 (c) i_2 (d) i_3 (e) i_4

(f) i_5 (g) i_6 (h) i_7 (i) i_8 (j) i_9

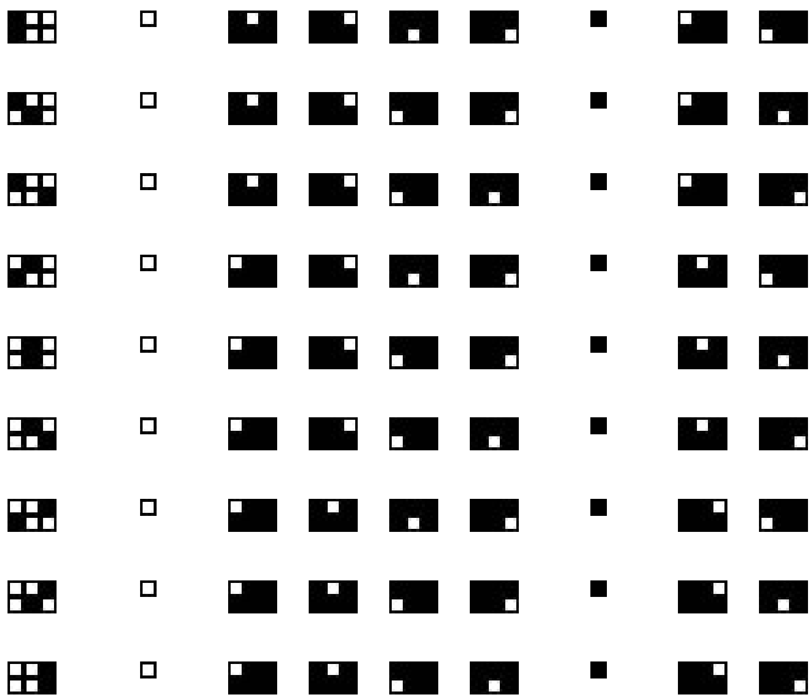
(k) i_{10} (l) i_{11} (m) i_{12} (n) i_{13} (o) i_{14}

FIG. 5.3: Conjunto de imagens $i_0, ..., i_{14}$ disponíveis para a escolha de Carol.

As construções possíveis de cada $B_p^{V_C}$, correspondente ao p-ésimo pixel de I_C^{tmp} segue a TAB. 5.5. Ela contém as 9 codificações que um bloco $B_p^{T_C^{tmp}}$ pode assumir. Caso o bloco $B_p^{V_C}$ represente um pixel branco em I_C^{tmp}, então deve haver 4 possibilidades para a sua construção, uma para cada subpixel branco em $B_p^{T_C^{tmp}}$.

TAB. 5.5: Construções de $B_p^{V_C}$ correspondente ao p-ésimo pixel em I_C^{tmp}.

$B_p^{T_C^{tmp}}$	p-ésimo pixel em I_C^{tmp}	$B_p^{V_C}$	p-ésimo pixel em I_C^{tmp}	$B_p^{V_C}$



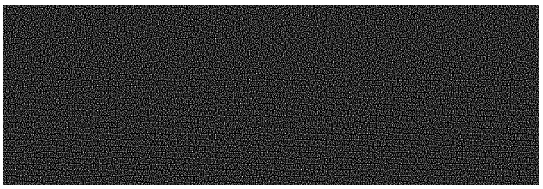
Neste caso, a cor do bloco resultante da sobreposição $B_p^{V_C} + B_p^{T_C^{tmp}}$ deve ser identificada pelo sistema visual de Carol como branca. De forma semelhante, caso o bloco $B_p^{V_C}$ represente um pixel preto em I_C^{tmp}, então deve haver 2 possibilidades para a sua construção, uma para cada subpixel preto em $B_p^{T_C^{tmp}}$. Neste caso, a cor do bloco resultante da sobreposição $B_p^{V_C} + B_p^{T_C^{tmp}}$ deve ser identificada pelo sistema visual de Carol como preta.

5.4 VERIFICAÇÃO DA INTEGRIDADE DE T_J ATRAVÉS DA AUTENTICAÇÃO DE $IV_I^1, ..., IV_I^{N^2-N}$

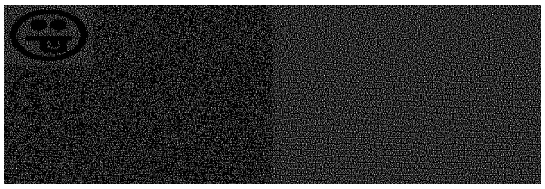
Conforme foi apresentado na Seção 5.1 e descrito em detalhes na Seção 5.2 e na Seção 5.3, no esquema de prevenção desenvolvido neste trabalho, cada participante P_i possui, além de sua transparência original T_i, uma transparência circular de verificação V_i, que deve ser utilizada por ele na verificação da integridade de cada transparência T_j, onde $j = 0, ..., n-1$, e $j \neq i$. Cada V_i é dividido em $n^3 - n^2$ regiões R_{xy}, onde $0 \leq x < n^2 - n$ e $0 \leq y < n$. A sobreposição $V_i + T_j$ reconstrói em cada R_{xy}, uma IV_i^z.

Portanto, após receber as transparências T_C e V_C, Carol se torna capaz de verificar a integridade das transparências de Alice e Bob, através do posicionamento de T_A ou T_B com V_C, seguido pelo deslocamento obtido pela rotação de T_A ou T_B sobre V_C nos ângulos $\frac{360^o}{z}$, onde $1 \leq z \leq n^2 - n = 6$. As rotações são definidas por $V_C \otimes T_j^{0^o}$, $V_C \otimes T_j^{60^o}$, $V_C \otimes T_j^{120^o}$, $V_C \otimes T_j^{180^o}$, $V_C \otimes T_j^{240^o}$ e $V_C \otimes T_j^{300^o}$.

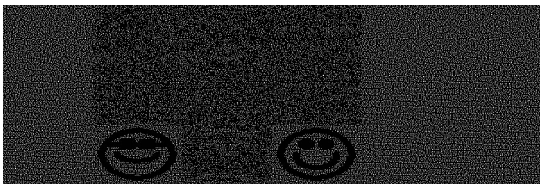
Caso as imagens de verificação $IV_C^1, ..., IV_C^6$ não sejam reconstruídas com clareza, Carol deve rejeitar T_A ou T_B, por considerar que a integridade da transparência foi violada, e possivelmente seja uma transparência falsa T'_A ou T'_B. Por outro lado, se a autenticação das imagens for efetuada com sucesso, Carol pode aceitar as sobreposições $T_A + T_C$ ou $T_A + T_B$ e concluir a fase de decodificação. O resultado de um experimento com a construção do novo esquema de prevenção é apresentado na FIG. 5.4.



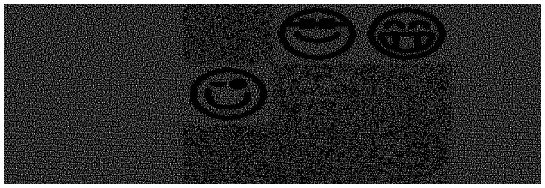
(a) V_C



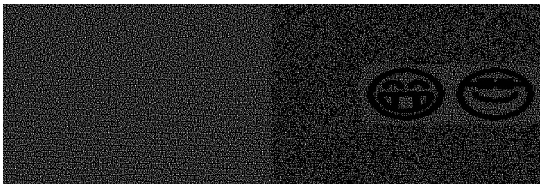
(b) $V_C \otimes T_A^{0^o}$



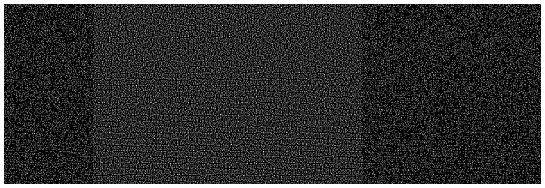
(c) $V_C \otimes T_A^{60^o}$



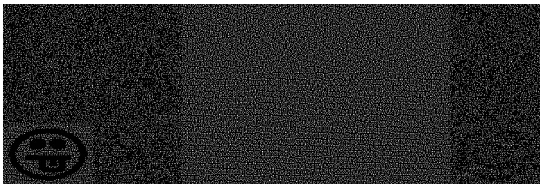
(d) $V_C \otimes T_A^{120^o}$



(e) $V_C \otimes T_A^{180^o}$



(f) $V_C \otimes T_A^{240^o}$



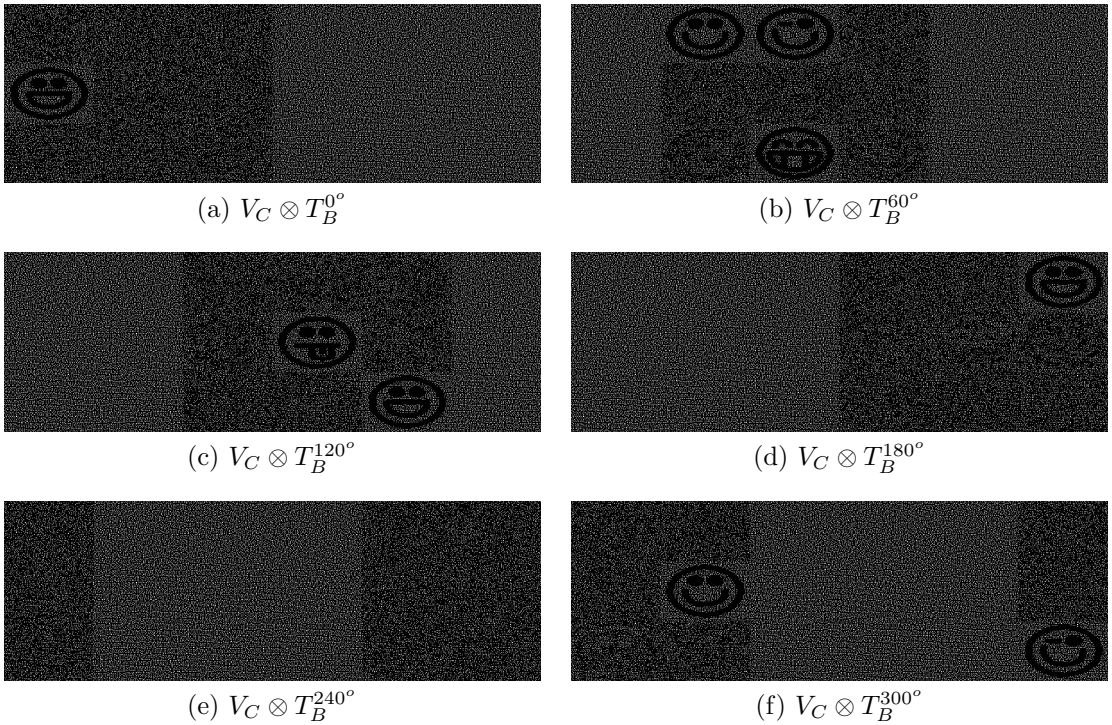
(g) $V_C \otimes T_A^{300^o}$

FIG. 5.4: Demonstrações de $V_C \otimes T_A^{0^o}$, $V_C \otimes T_A^{60^o}$, $V_C \otimes T_A^{120^o}$, $V_C \otimes T_A^{180^o}$, $V_C \otimes T_A^{240^o}$ e $V_C \otimes T_A^{300^o}$ no novo esquema de prevenção.

A FIG. 5.4 contém a transparência circular de verificação V_C e as sobreposições realizadas através das 6 rotações entre T_A e V_C. A transparência circular de verificação V_C, que pode ser visualizada no item (a), foi construída a partir de $i_0, ..., i_5$. Esta transparência de verificação também possui 300×900 pixels.

As sobreposições $V_C \otimes T_A^{0^o}$, $V_C \otimes T_A^{60^o}$, $V_C \otimes T_A^{120^o}$, $V_C \otimes T_A^{180^o}$, $V_C \otimes T_A^{240^o}$ e $V_C \otimes T_A^{300^o}$ podem ser visualizadas nos itens (b), (c), (d), (e), (f) e (g), respectivamente. A sobreposição $V_C \otimes T_A^{0^o}$ define a reconstrução de i_5 na região R_{00} de V_C. De forma semelhante, a sobreposição $V_C \otimes T_A^{60^o}$ define em V_C as reconstruções de i_0 e i_4 nas regiões R_{32} e R_{12}, respectivamente. A sobreposição $V_C \otimes T_A^{120^o}$ define em V_C as reconstruções de i_2, i_3 e i_4, nas regiões R_{40}, R_{21} e R_{30}, respectivamente.

Ainda na FIG. 5.4, a sobreposição $V_C \otimes T_A^{180^o}$ define em V_C as reconstruções de i_2 e i_4 nas regiões R_{41} e R_{51}, respectivamente. A sobreposição $V_C \otimes T_A^{240^o}$ não define a reconstrução de qualquer imagem de verificação em V_C. Finalmente, a sobreposição $V_C \otimes T_A^{300^o}$ define a reconstrução de i_5 na região R_{02} de V_C. Na FIG. 5.5 é apresentada a outra parte do experimento, que está relacionada com as sobreposições de verificação entre V_C e T_B.



(a) $V_C \otimes T_B^{0^o}$ (b) $V_C \otimes T_B^{60^o}$

(c) $V_C \otimes T_B^{120^o}$ (d) $V_C \otimes T_B^{180^o}$

(e) $V_C \otimes T_B^{240^o}$ (f) $V_C \otimes T_B^{300^o}$

FIG. 5.5: Demonstrações de $V_C \otimes T_B^{0^o}$, $V_C \otimes T_B^{60^o}$, $V_C \otimes T_B^{120^o}$, $V_C \otimes T_B^{180^o}$, $V_C \otimes T_B^{240^o}$ e $V_C \otimes T_B^{300^o}$ no novo esquema de prevenção.

A FIG. 5.5 contém as sobreposições realizadas através das 6 rotações entre T_B e V_C. As sobreposições $V_C \otimes T_B^{0^o}$, $V_C \otimes T_B^{60^o}$, $V_C \otimes T_B^{120^o}$, $V_C \otimes T_B^{180^o}$, $V_C \otimes T_B^{240^o}$ e $V_C \otimes T_B^{300^o}$ podem ser visualizadas nos itens (a), (b), (c), (d), (e) e (f), respectivamente. A sobreposição $V_C \otimes T_B^{0^o}$ define a reconstrução de i_1 na região R_{01} de V_C. De forma semelhante, a sobreposição $V_C \otimes T_B^{60^o}$ define em V_C as reconstruções de i_0, i_2 e i_3 nas regiões R_{10}, R_{22} e R_{20}, respectivamente.

Ainda na FIG. 5.5, a sobreposição $V_C \otimes T_B^{120^o}$ define em V_C as reconstruções de i_1 e i_5 nas regiões R_{42} e R_{31}, respectivamente. Da mesma forma, a sobreposição $V_C \otimes T_B^{180^o}$ define a reconstrução de i_1 na região R_{50} de V_C. A sobreposição $V_C \otimes T_B^{240^o}$ não define a reconstrução de qualquer imagem de verificação em V_C. Finalmente, a sobreposição $V_C \otimes T_B^{300^o}$ define em V_C as reconstruções de i_0 e i_3, nas regiões R_{11} e R_{52}, respectivamente.

5.5 MÓDULO DE VALIDAÇÃO DAS IMAGENS DE VERIFICAÇÃO $IV_0^1, ..., IV_{N-1}^{N^2-N}$

Um módulo de validação das imagens de verificação foi incluído no novo esquema de prevenção. Este módulo é capaz de limitar a quantidade de bits pretos contidos em cada imagem de verificação IV_i^z, onde $0 \leq i \leq n$ e $1 \leq z \leq n^2 - n$. O módulo deve ser capaz de modificar qualquer imagem de verificação IV_i^z que possua a quantidade de pixels pretos superior ao limite estabelecido. Esta função tornaria dispensável a possibilidade de rejeição das imagens reprovadas na validação.

O módulo é ativado no momento em que o participante P_i envia ao esquema, através de canais seguros, a sua coleção CIV_i de imagens de verificação escolhidas. Neste momento, o módulo deve realizar uma simples contagem dos pixels pretos em cada imagem de verificação IV_i^z. Se a quantidade for superior a uma porcentagem predefinida do total de pixels da imagem, então o módulo deve inverter a cor de todos os pixels de IV_i^z, da seguinte forma: os pixels pretos se tornarão brancos e os pixels brancos se tornarão pretos. Alguns exemplos de execução do módulo de validação com o limite estabelecido para 50% serão apresentados na TAB. 5.6.

A imagem de verificação inicial é definida por IV_I. A imagem resultante após o processamento do módulo de validação é definida por IV_R. As duas imagens IV_I e IV_R possuem em todos os casos $50 \times 50 = 2500$ pixels. Na primeira validação apresentada na TAB. 5.6, foi definido o logo do IME para ser a IV_I. O módulo verificou que esta imagem de verificação possui 1640 pixels brancos e 860 pixels pretos. Neste caso, a imagem IV_I passou na validação e será utilizada IV_R no formato original.

TAB. 5.6: Validações de algumas imagens de verificação.

IV_I	$\rightarrow$	IV_R	IV_I	$\rightarrow$	IV_R
					
					

Na segunda validação, foi definida uma imagem com as letras IME para ser IV_I. O módulo verificou que esta imagem possui 1046 pixels brancos e 1454 pixels pretos. Neste caso, a imagem IV_I não passou na validação e será utilizada IV_R no formato invertido. Na terceira validação, foi definido um *smile* de cor predominantemente branca para ser IV_I. O módulo verificou que esta imagem possui 1631 pixels brancos e 869 pixels pretos. Neste caso, a imagem IV_I passou na validação e será utilizada IV_R no formato original.

Finalmente, na quarta validação apresentada na TAB. 5.6, foi definido um *smile* de cor predominantemente preta para ser IV_I. O módulo verificou que esta imagem de verificação possui 876 pixels brancos e 1624 pixels pretos. Neste caso, a imagem IV_I não passou na validação e será utilizada IV_R no formato invertido.

5.6 SUPORTE AOS ASPECTOS DE SEGURANÇA

Neste Capítulo, foi apresentado o esquema de prevenção contra fraude em Criptografia Visual desenvolvido neste trabalho, através de uma exposição das principais definições sobre a construção e a forma de utilização das transparências disponibilizadas para os participantes Alice, Bob e Carol. O experimento apresentado na Seção 5.4 demonstrou o funcionamento do processo de verificação das transparências T_A e T_B realizado por Carol, que utilizou o novo esquema de prevenção.

No entanto, não será suficiente detectar a fraude convencional definida na Seção 3.2 e demonstrada na Seção 3.3. A análise realizada na Seção 4.6 forneceu uma base sólida para a construção do novo esquema de prevenção. Os aspectos de segurança relacionados com as vulnerabilidades identificadas nos esquemas HCT e HT tornaram-se requisitos indispensáveis no projeto do novo esquema. No Capítulo 6, os aspectos de segurança do novo esquema de prevenção serão discutidos.

6 ASPECTOS DE SEGURANÇA DA NOVA PREVENÇÃO

O objetivo deste Capítulo é apresentar uma discussão sobre os aspectos de segurança relacionados com o novo esquema de prevenção introduzido no Capítulo 5. É necessário que o novo esquema forneça suporte sobre esses aspectos, que podem ser resumidos em: detectar a fraude e a oferecer segurança contra os três ataques aos esquemas HCT e HT. Este Capítulo está organizado da seguinte forma. Na Seção 6.1 será apresentada uma adaptação nas definições sobre fraude discutidas no Capítulo 3, com o objetivo de demonstrar um ataque sobre o novo esquema. Nesta Seção, também será apresentado um experimento que simula a detecção da fraude, o que garante o suporte ao primeiro aspecto de segurança. Na Seção 6.2, será apresentada uma análise sobre a incapacidade dos ataques conhecidos diante do novo esquema de prevenção, através da demonstração de um experimento que combina as técnicas conhecidas, o que garante o suporte sobre os aspectos de segurança restantes.

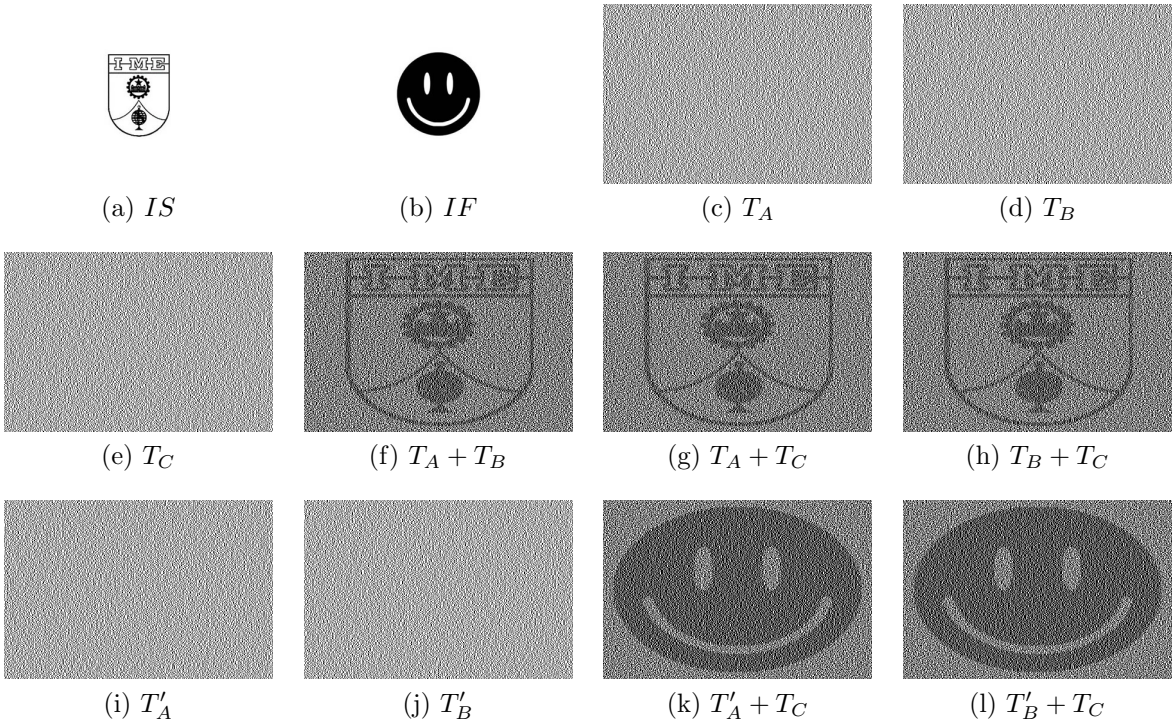
6.1 PROCEDIMENTO PARA DETECÇÃO DA FRAUDE

O procedimento para realizar a fraude no novo esquema é semelhante ao descrito no Capítulo 3. Alice, Bob e Carol devem receber T_A, T_B e T_C, respectivamente. Supondo que o desejo de Alice e Bob seja enganar Carol, então eles devem construir T'_A e T'_B através das transformações $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$, com base no bloco $B_p^{T_C}$ que Alice e Bob são capazes de prever. Cada transformação deve ser realizada com base no p-ésimo pixel da IS, considerando a estrutura de cada bloco no novo esquema, de acordo com as definições apresentadas na Seção 5.2. Desta forma, cada uma das sobreposições $T'_A + T_C$ e $T'_B + T_C$ reconstruirá a imagem falsa IF.

Na TAB. 5.1 e na TAB. 5.2, são apresentadas todas as possibilidades de construção, caso o p-ésimo pixel da imagem secreta IS seja branco. Se o p-ésimo pixel for branco na IS e também na IF, então $B_p^{T_A}$ será igual a $B_p^{T'_A}$ e $B_p^{T_B}$ será igual a $B_p^{T'_B}$, pois o p-ésimo pixel é branco da IS e na IF. Na TAB. 5.3 e na TAB. 5.4, são apresentadas todas as possibilidades de construção, caso o p-ésimo pixel da imagem secreta IS seja preto. Se o p-ésimo pixel for preto na IS e também na IF, então $B_p^{T_A}$ será igual a $B_p^{T'_A}$ e $B_p^{T_B}$ será igual a $B_p^{T'_B}$, pois o p-ésimo pixel é preto na IS e na IF.

Caso o p-ésimo pixel seja branco na IS e preto na IF, então Alice e Bob devem comparar $B_p^{T_A}$ e $B_p^{T_B}$ e inferir sobre $B_p^{T_C}$, pois todas as linhas em $C_0^0(S_0)$ ou $C_0^1(S_0)$ são iguais. Eles devem transformar $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ para que o bloco resultante de $B_p^{T'_A} + B_p^{T_C}$ e $B_p^{T'_B} + B_p^{T_C}$ seja preto. Para isso, eles devem identificar a linha do bloco correspondente a $C_0^0(S_0)$ ou $C_0^1(S_0)$, onde a posição do pixel preto é igual em $B_p^{T'_A}$ e $B_p^{T'_B}$ e repetir nesta linha o procedimento do segundo caso da TAB. 3.2.

Se o p-ésimo pixel for preto na IS e branco na IF, então Alice e Bob devem comparar $B_p^{T_A}$ e $B_p^{T_B}$ e inferir sobre $B_p^{T_C}$, pois todas as linhas em C_1^0 ou C_1^1 são diferentes. Eles devem transformar $B_p^{T_A} \rightarrow B_p^{T'_A}$ e $B_p^{T_B} \rightarrow B_p^{T'_B}$ para que o bloco resultante de $B_p^{T'_A} + B_p^{T_C}$ e $B_p^{T'_B} + B_p^{T_C}$ seja branco. Para isso, eles devem identificar a linha do bloco correspondente a $C_0^0(S_0)$ ou $C_0^1(S_0)$, onde a posição do pixel preto é igual em $B_p^{T'_A}$ e $B_p^{T'_B}$ e repetir nesta linha o procedimento descrito no segundo caso da TAB. 3.2. Para isso, eles devem escolher aleatoriamente uma linha do bloco correspondente a C_1^0 ou C_1^1, onde a posição do pixel preto é diferente em $B_p^{T'_A}$ e $B_p^{T'_B}$ e repetir nesta linha o procedimento do primeiro caso da TAB. 3.3. O experimento que demonstra a execução e a detecção da fraude é apresentado na FIG. 6.1, na FIG. 6.2, na FIG. 6.3, na FIG. 6.4 e na FIG. 6.5.



(a) IS (b) IF (c) T_A (d) T_B

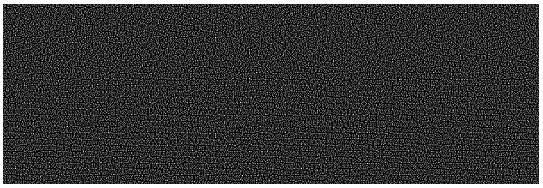
(e) T_C (f) $T_A + T_B$ (g) $T_A + T_C$ (h) $T_B + T_C$

(i) T'_A (j) T'_B (k) $T'_A + T_C$ (l) $T'_B + T_C$

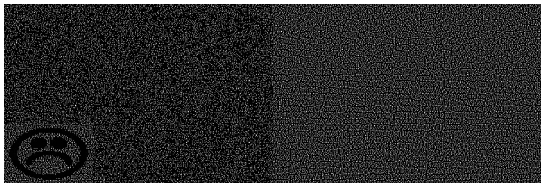
FIG. 6.1: Demonstração de $T'_A + T_C = IF$ e $T'_B + T_C = IF$ no novo esquema de prevenção.

Na FIG. 6.1, a imagem secreta IS pode ser visualizada no item (a). Foi definido o logo do IME com 150×150 pixels, para ser a IS. A imagem falsa IF escolhida por Alice e Bob pode ser visualizada no item (b). Foi definido um *smile* de cor predominantemente preta com 150×150 pixels, para ser a IF. O conjunto de imagens de verificação escolhidas por Carol é composto por $i_6, ..., i_{11}$, de acordo com a FIG. 5.3. As três transparências originais T_A, T_B e T_C, que podem ser visualizadas nos itens (c), (d) e (e), respectivamente, foram construídas a partir da IS. Cada T_i possui 300×450 pixels.

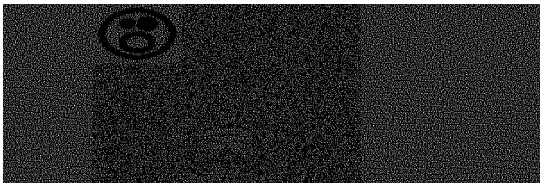
As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$, que podem ser visualizadas nos itens (f), (g) e (h), respectivamente, definem a reconstrução da IS. As duas transparências falsas T'_A e T'_B, que podem ser visualizadas nos (i) e (j), respectivamente, foram construídas a partir da IF. Cada T'_i possui 150×450 pixels. As sobreposições $T'_A + T_C$ e $T'_B + T_C$, que podem ser visualizadas nos itens (k) e (l), respectivamente, reconstroem a IF.



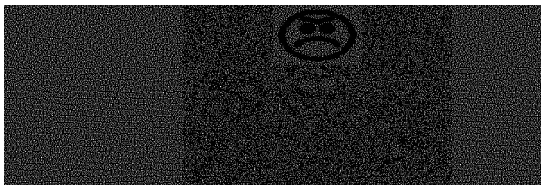
(a) V_C



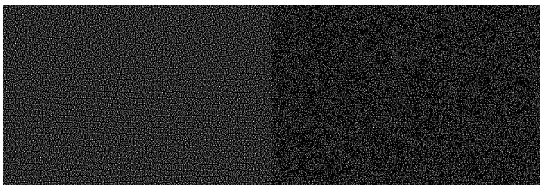
(b) $V_C \otimes T_A^{0^o}$



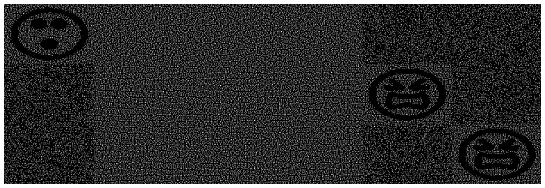
(c) $V_C \otimes T_A^{60^o}$



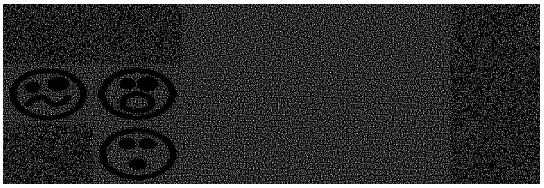
(d) $V_C \otimes T_A^{120^o}$



(e) $V_C \otimes T_A^{180^o}$



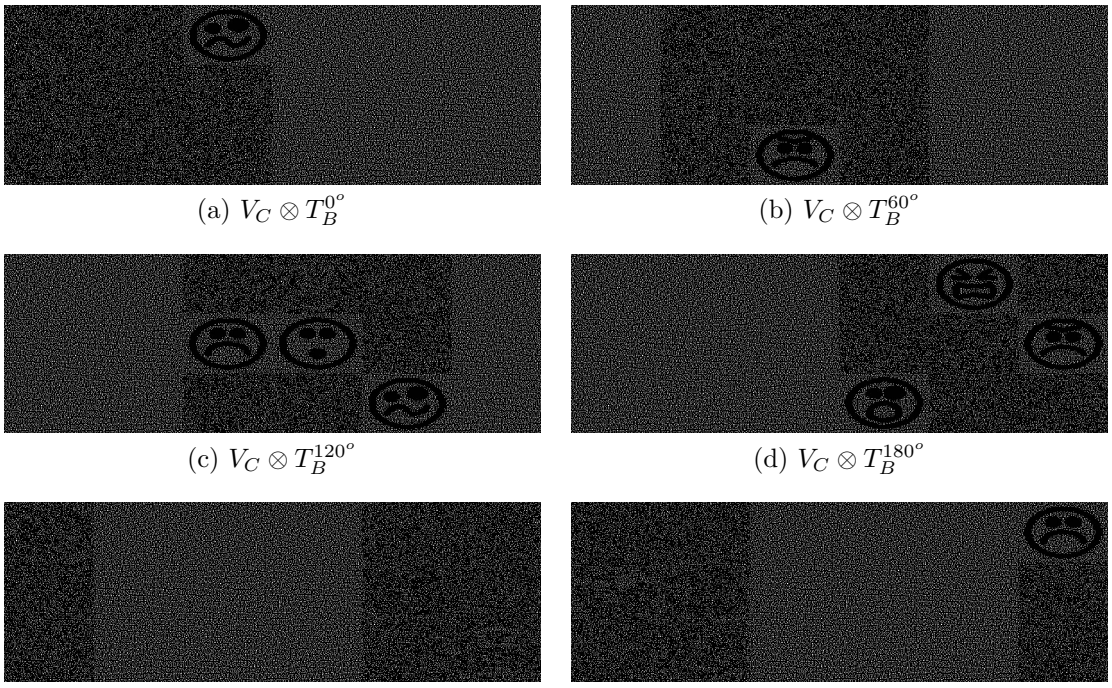
(f) $V_C \otimes T_A^{240^o}$



(g) $V_C \otimes T_A^{300^o}$

FIG. 6.2: Sobreposições $V_C \otimes T_A^{0^o}$, $V_C \otimes T_A^{60^o}$, $V_C \otimes T_A^{120^o}$, $V_C \otimes T_A^{180^o}$, $V_C \otimes T_A^{240^o}$ e $V_C \otimes T_A^{300^o}$.

A FIG. 6.2 contém as sobreposições obtidas através das rotações entre T_A e V_C. A transparência V_C e as sobreposições $V_C \otimes T_A^{0^o}$, $V_C \otimes T_A^{60^o}$, $V_C \otimes T_A^{120^o}$, $V_C \otimes T_A^{180^o}$, $V_C \otimes T_A^{240^o}$ e $V_C \otimes T_A^{300^o}$ podem ser visualizadas nos itens (a), (b), (c), (d), (e), (f) e (g), respectivamente. A sobreposição $V_C \otimes T_A^{0^o}$ define a reconstrução de i_7. A sobreposição $V_C \otimes T_A^{60^o}$ define a reconstrução de i_{10}. A sobreposição $V_C \otimes T_A^{120^o}$ define a reconstrução de i_9. A sobreposição $V_C \otimes T_A^{180^o}$ não define a reconstrução qualquer imagem de verificação. A sobreposição $V_C \otimes T_A^{240^o}$ define a reconstrução de i_8 e i_{11}. A sobreposição $V_C \otimes T_A^{300^o}$ define a reconstrução de i_6, i_{10} e i_{11}.



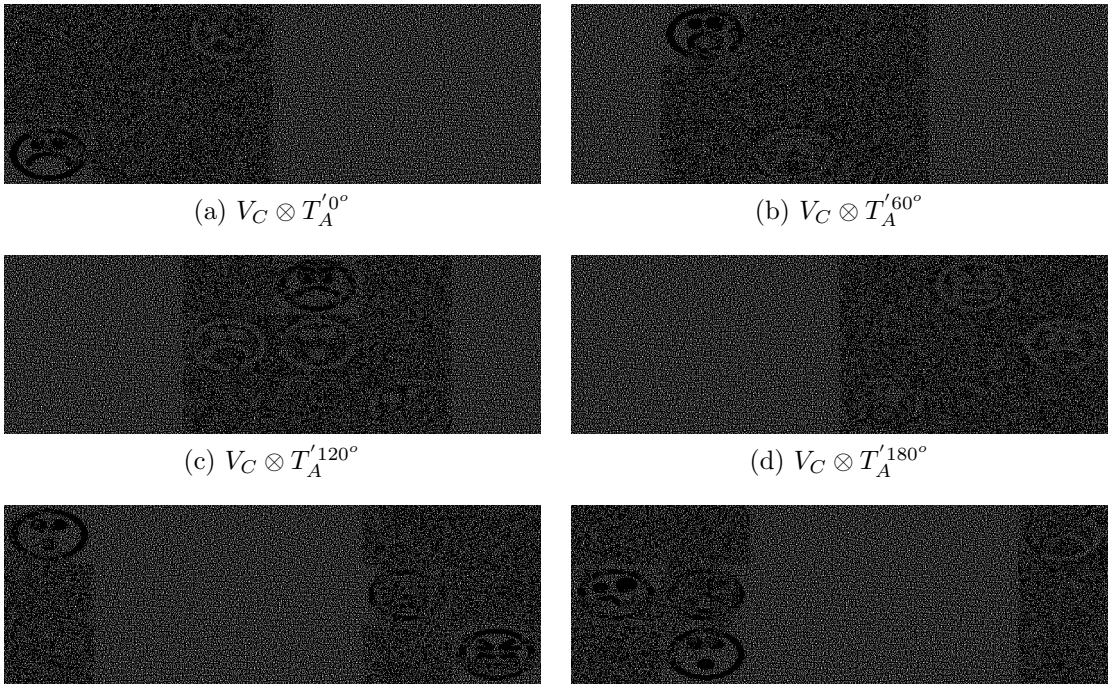
(a) $V_C \otimes T_B^{0^o}$ (b) $V_C \otimes T_B^{60^o}$

(c) $V_C \otimes T_B^{120^o}$ (d) $V_C \otimes T_B^{180^o}$

(e) $V_C \otimes T_B^{240^o}$ (f) $V_C \otimes T_B^{300^o}$

FIG. 6.3: Sobreposições $V_C \otimes T_B^{0^o}$, $V_C \otimes T_B^{60^o}$, $V_C \otimes T_B^{120^o}$, $V_C \otimes T_B^{180^o}$, $V_C \otimes T_B^{240^o}$ e $V_C \otimes T_B^{300^o}$.

A FIG. 6.3 contém as sobreposições obtidas através das rotações entre T_B e V_C. As sobreposições $V_C \otimes T_B^{0^o}$, $V_C \otimes T_B^{60^o}$, $V_C \otimes T_B^{120^o}$, $V_C \otimes T_B^{180^o}$, $V_C \otimes T_B^{240^o}$ e $V_C \otimes T_B^{300^o}$ podem ser visualizadas nos itens (a), (b), (c), (d), (e) e (f), respectivamente. A sobreposição $V_C \otimes T_B^{0^o}$ define a reconstrução de i_6. A sobreposição $V_C \otimes T_B^{60^o}$ define a reconstrução de i_9. A sobreposição $V_C \otimes T_B^{120^o}$ define a reconstrução de i_6, i_7 e i_{11}. A sobreposição $V_C \otimes T_B^{180^o}$ define a reconstrução de i_8, i_9 e i_{10}. A sobreposição $V_C \otimes T_B^{240^o}$ não define a reconstrução qualquer imagem de verificação. A sobreposição $V_C \otimes T_B^{300^o}$ define a reconstrução de i_7. Na FIG. 6.2 e na FIG. 6.3 foi demonstrado o processo de verificação de T_A e T_B.



(a) $V_C \otimes T_A^{'0^o}$ (b) $V_C \otimes T_A^{'60^o}$

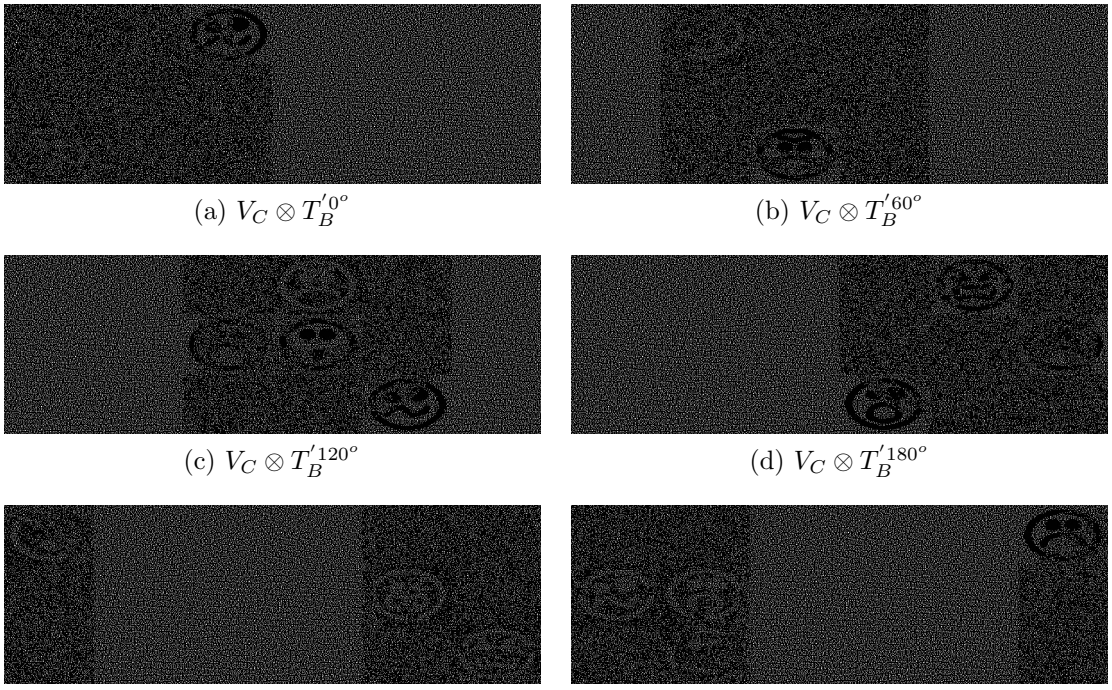
(c) $V_C \otimes T_A^{'120^o}$ (d) $V_C \otimes T_A^{'180^o}$

(e) $V_C \otimes T_A^{'240^o}$ (f) $V_C \otimes T_A^{'300^o}$

FIG. 6.4: Sobreposições $V_C \otimes T_A^{'0^o}$, $V_C \otimes T_A^{'60^o}$, $V_C \otimes T_A^{'120^o}$, $V_C \otimes T_A^{'180^o}$, $V_C \otimes T_A^{'240^o}$ e $V_C \otimes T_A^{'300^o}$.

A FIG. 6.4 contém as sobreposições obtidas através das rotações entre T'_A e V_C. As sobreposições $V_C \otimes T_A^{0^o}$, $V_C \otimes T_A^{'60^o}$, $V_C \otimes T_A^{'120^o}$, $V_C \otimes T_A^{'180^o}$, $V_C \otimes T_A^{'240^o}$ e $V_C \otimes T_A^{'300^o}$ podem ser visualizadas em (a), (b), (c), (d), (e) e (f), respectivamente. A sobreposição $V_C \otimes T_A^{'0^o}$ não define com clareza a reconstrução de i_7. A sobreposição $V_C \otimes T_A^{'60^o}$ não define com clareza a reconstrução de i_{10}. A sobreposição $V_C \otimes T_A^{'120^o}$ não define com clareza a reconstrução de i_9. A sobreposição $V_C \otimes T_A^{'180^o}$ não define a reconstrução qualquer imagem de verificação. A sobreposição $V_C \otimes T_A^{'240^o}$ não define com clareza a reconstrução de i_8 e i_{11}. A sobreposição $V_C \otimes T_A^{'300^o}$ não define com clareza a reconstrução de i_6, i_{10} e i_{11}.

A FIG. 6.5 contém as sobreposições realizadas através das 6 rotações entre T'_B e V_C. As sobreposições $V_C \otimes T_B^{'0^o}$, $V_C \otimes T_B^{'60^o}$, $V_C \otimes T_B^{'120^o}$, $V_C \otimes T_B^{'180^o}$, $V_C \otimes T_B^{'240^o}$ e $V_C \otimes T_B^{'300^o}$ podem ser visualizadas em (a), (b), (c), (d), (e) e (f), respectivamente. A sobreposição $V_C \otimes T_B^{'0^o}$ não define com clareza a reconstrução de i_6. A sobreposição $V_C \otimes T_B^{'60^o}$ não define com clareza a reconstrução de i_9. A sobreposição $V_C \otimes T_B^{'120^o}$ não define com clareza a reconstrução de i_6, i_7 e i_{11}. A sobreposição $V_C \otimes T_B^{'180^o}$ não define com clareza a reconstrução de i_8, i_9 e i_{10}. A sobreposição $V_C \otimes T_B^{'240^o}$ não define a reconstrução de



(a) $V_C \otimes T_B^{'0^o}$ (b) $V_C \otimes T_B^{'60^o}$

(c) $V_C \otimes T_B^{'120^o}$ (d) $V_C \otimes T_B^{'180^o}$

(e) $V_C \otimes T_B^{'240^o}$ (f) $V_C \otimes T_B^{'300^o}$

FIG. 6.5: Sobreposições $V_C \otimes T_B^{'0^o}$, $V_C \otimes T_B^{'60^o}$, $V_C \otimes T_B^{'120^o}$, $V_C \otimes T_B^{'180^o}$, $V_C \otimes T_B^{'240^o}$ e $V_C \otimes T_B^{'300^o}$.

qualquer imagem de verificação. A sobreposição $V_C \otimes T_B^{'300^o}$ não define com clareza a reconstrução de i_7. Na FIG. 6.4 e na FIG. 6.5 foi demonstrado o processo de verificação das transparências falsas de Alice e Bob, T'_A e T'_B, respectivamente.

6.2 RESISTÊNCIA CONTRA OS ATAQUES CONHECIDOS

Os aspectos de segurança do novo esquema de prevenção devem incluir, além da capacidade de detecção a fraude, cuja demonstração foi apresentada na Seção 6.1, a resistência contra os três ataques aos esquemas HCT e HT. O primeiro ataque identificou uma vulnerabilidade do HCT e foi demonstrado na Seção 4.2. A base para este ataque está relacionada com a verificação parcial da integridade de T_A e T_B, que é realizada pelas sobreposições $V_C + T_A$ e $V_C + T_B$. Desta forma, Alice pode construir T'_A modificando os blocos localizados fora de R_{CA} e Bob pode construir T'_B modificando os blocos localizados fora de R_{CB}. O novo esquema de prevenção contra fraude definido no Capítulo 5 não é vulnerável contra este ataque, pois a integridade de cada transparência T_A, T_B, T'_A ou T'_B é completamente verificada por V_C.

O segundo ataque também identificou uma vulnerabilidade do HCT e foi demonstrado na Seção 4.3. Este é o ataque mais importante dos três. Um $ABCPS$ não deve fornecer em T_i e V_i informações suficientes para que um participante qualquer P_i obtenha a IS individualmente. Na Seção 4.3 foi definido que Alice realizaria este ataque. O método que Alice tem à sua disposição para realizar este ataque é a escolha das imagens de verificação com o maior número possível de pixels pretos. No entanto, esta possibilidade foi reduzida por um módulo adicionado ao novo esquema, descrito na Seção 5.5. Este módulo é capaz de limitar a quantidade de bits pretos contidos em cada imagem de verificação informada, através da inversão das cores de todos os pixeis de uma imagem que exceda um limite pré-definido da quantidade máxima de pixels pretos.

Além disso, no HCT Alice conhece a imagem de verificação que deve ser revelada nas regiões R_{AB} e R_{AC} em V_A. No novo esquema de prevenção, Alice seria obrigada a encontrar as permutações realizadas no posicionamento das imagens de verificação por força bruta. É necessário definir a quantidade máxima de pixels pretos supondo que Alice conheça as permutações utilizadas na construção de V_A. A FIG. 6.6 contém um pequeno grupo de imagens com 50×50 pixels que serão utilizadas nos próximos experimentos como imagens de verificação disponíveis para a escolha de Alice.

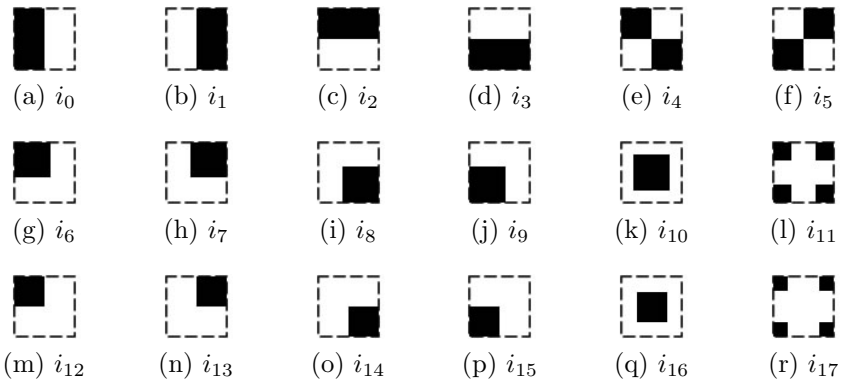
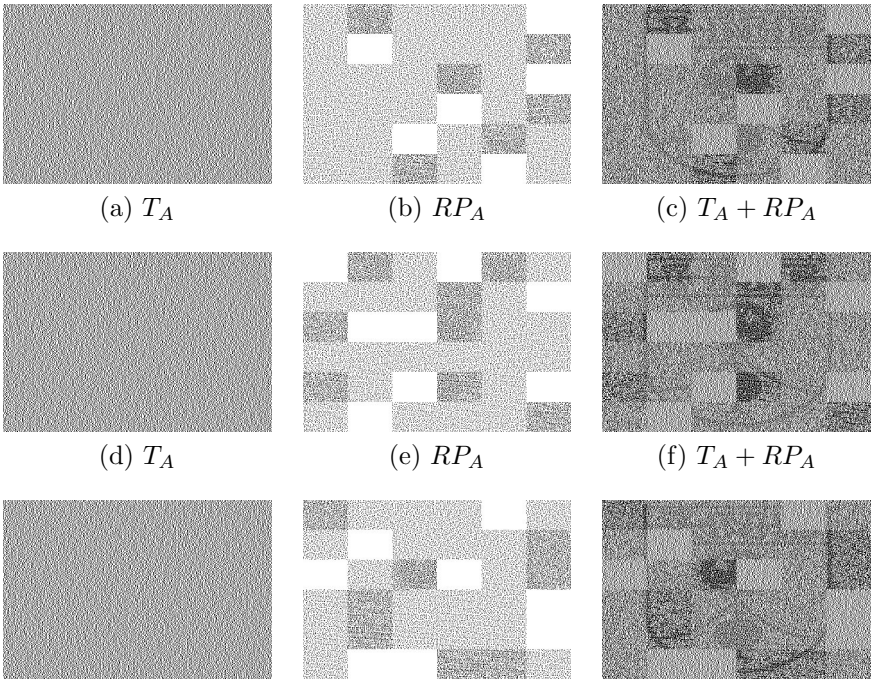


FIG. 6.6: Conjunto de imagens $i_0, ..., i_{17}$ disponíveis para a escolha de Alice.

Os subconjuntos de imagens $i_0, ..., i_5$, $i_6, ..., i_{11}$ e $i_{12}, ..., i_{17}$ possuem 50%, 25% e 35% de pixels pretos, respectivamente. Alice não pode controlar o posicionamento das imagens nas regiões de V_A. No entanto, ela sabe que há duas regiões em V_A que estão relacionadas com a mesma região da IS. A interseção entre essas regiões sobrepostas com a região correspondente em V_A poderia revelar parte da IS. Caso Alice descubra através de força bruta os posicionamentos das imagens de verificação em V_A e das regiões relacionadas

em T_B e T_C, então ela será capaz de realizar um ataque ao novo esquema de prevenção, que combina as técnicas utilizadas no segundo ataque, realizado contra o HCT, por explorar a quantidade máxima de pixels pretos e no terceiro ataque, realizado contra o HT, por explorar o uso de imagens complementares. Os resultados de três experimentos que demonstram a execução deste ataque ao novo esquema de prevenção serão apresentados na FIG. 6.7, na FIG. 6.8 e na FIG. 6.9.



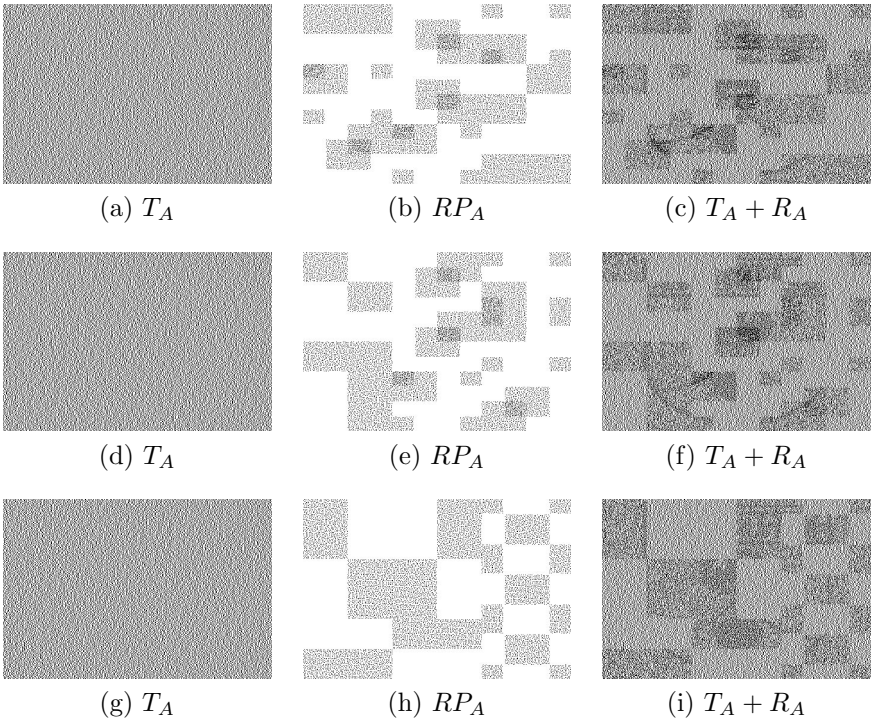
(a) T_A (b) RP_A (c) $T_A + RP_A$

(d) T_A (e) RP_A (f) $T_A + RP_A$

(g) T_A (h) RP_A (i) $T_A + RP_A$

FIG. 6.7: Demonstrações de $T_A + RP_A = IS$ com 50% de pixels pretos nas imagens de verificação escolhidas para o ataque.

Cada um dos experimentos foi executado três vezes, por conta de possíveis variações nos resultados do ataque, causadas pela aleatoriedade na definição do posicionamento das regiões em V_A. Nos três experimentos foi definido o logo do IME com 150×150 pixels, para ser a IS. Na FIG. 6.7, na FIG. 6.8 e na FIG. 6.9, a transparência T_A em cada execução pode ser visualizada em (a), (d) e (g). Cada transparência T_A possui 300×450 pixels. A transparência RP_A, construída por Alice com base no posicionamento das imagens de verificação, pode ser visualizada em (b), (e) e (h). Cada RP_A também possui 300×450 pixels. As regiões relacionadas com as áreas com pixels brancos das imagens de verificação não são utilizadas na reconstrução.



(a) T_A (b) RP_A (c) $T_A + R_A$

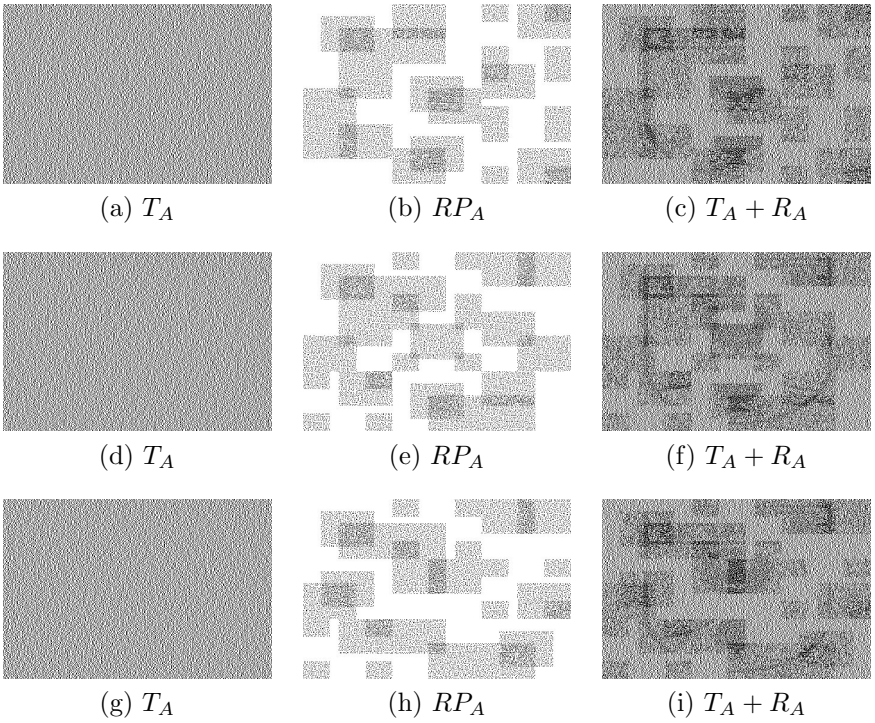
(d) T_A (e) RP_A (f) $T_A + R_A$

(g) T_A (h) RP_A (i) $T_A + R_A$

FIG. 6.8: Demonstrações de $T_A + RP_A \neq IS$ com 25% de pixels pretos nas imagens de verificação escolhidas para o ataque.

No primeiro experimento, demonstrado na FIG. 6.7, o subconjunto de imagens de verificação escolhidas por Alice é formado por $i_0, ..., i_5$. Cada uma dessas imagens é composta por 50% de pixels pretos. No segundo experimento, demonstrado na FIG. 6.8, o subconjunto de imagens de verificação escolhidas por Alice é formado por $i_6, ..., i_{11}$. Cada uma dessas imagens é composta por 25% de pixels pretos. No terceiro experimento, demonstrado na FIG. 6.9, o subconjunto de imagens de verificação escolhidas por Alice é formado por $i_{12}, ..., i_{17}$. Cada uma dessas imagens é composta por 35% de pixels pretos.

O ajuste correto da quantidade máxima de pixels pretos no módulo de validação tornará o esquema seguro contra este ataque. É possível concluir com base no experimento demonstrado na FIG. 6.7, que o ataque definido nesta Seção pode revelar informações suficientes para que Alice conclua que a IS é o logo do IME, quando o limite máximo de pixels pretos no módulo de validação é de 50%. O experimento demonstrado na FIG. 6.8 permite concluir que o ataque definido nesta Seção não revela informações suficientes para que Alice conclua que a IS é o logo do IME, quando o limite máximo de pixels pretos no módulo de validação é de 25%.



(a) T_A (b) RP_A (c) $T_A + R_A$

(d) T_A (e) RP_A (f) $T_A + R_A$

(g) T_A (h) RP_A (i) $T_A + R_A$

FIG. 6.9: Demonstrações de $T_A + RP_A \neq IS$ com 35% de pixels pretos nas imagens de verificação escolhidas para o ataque.

No entanto, é desejável um percentual maior de pixels pretos nas imagens de verificação para aumentar a possibilidade de detecção da fraude. O experimento demonstrado na FIG. 6.9 permite concluir que o ataque definido nesta Seção não revela informações suficientes para que Alice conclua que a IS é o logo do IME, quando o limite máximo de pixels pretos no módulo de validação é de aproximadamente 35%. Este ajuste realizado especificamente sobre o logo do IME como IS, impediu que Alice fosse bem sucedida neste ataque.

O terceiro ataque foi demonstrado na Seção 4.5. Este ataque é específico sobre o esquema HT que utiliza nos blocos subpixels de autenticação independentes dos subpixels de reconstrução da IS. Os experimentos apresentados na FIG. 6.7, na FIG. 6.8 e na FIG. 6.9 demonstraram que as permutações utilizadas na definição do posicionamento das imagens de verificação inviabilizaram a combinação de imagens complementares, pois elas não foram definidas em posições favoráveis à identificação das informações da vítima. Ainda que o resultado fosse favorável, seriam reveladas somente as posições dos subpixels da transparência original da vítima. Este ataque não se aplica ao novo esquema, pois sua estrutura não é baseada na separação dos subpixels de autenticação e de reconstrução.

7 CONCLUSÃO

Neste trabalho, foi apresentada a construção de um esquema de prevenção contra fraude em Criptografia Visual que fornece a qualquer participante a capacidade de detectar a fraude, caso desconfie que os outros participantes não sejam honestos, por suspeitar que as suas transparências não sejam originais e que a imagem reconstruída após uma sobreposição não seria verdadeira. Uma análise sobre os ataques realizados contra o HCT e o HT também foi apresentada, com base na demonstração através de experimentos das vulnerabilidades exploradas por eles e na apresentação de sugestões sobre possíveis correções aos esquemas. Esta análise sobre os ataques às vulnerabilidades dos esquemas HCT e HT forneceu a base do projeto para o desenvolvimento de um novo esquema de prevenção contra fraude em Criptografia Visual.

A estrutura básica deste projeto, que forneceu suporte aos aspectos de segurança definidos neste trabalho como a capacidade de detecção da fraude e a resistência sobre os ataques conhecidos aos esquemas HCT e HT, pode ser resumida da seguinte forma. O desenvolvimento de uma versão adaptada do esquema que codifica múltiplas imagens, construído por SHYU et al. (2007), forneceu o suporte à segurança diante do ataque definido por HU e TZENG (2007) contra o esquema de prevenção HCT, através da capacidade de verificação da integridade de toda a extensão das transparências dos outros participantes, com base na utilização de transparências circulares.

A adição de um módulo de validação ao projeto forneceu o suporte à segurança contra o ataque definido por LIU, WU e LIN (2011) ao esquema de prevenção HCT, através da capacidade de limitar a quantidade de pixels pretos nas imagens de verificação informadas pelos participantes. Um mecanismo de permutação do posicionamento das imagens que devem ser autenticadas durante o processo de verificação das transparências ofereceu o suporte à segurança contra o ataque definido por LIU, WU e LIN (2011) ao esquema HT, pois ele inviabilizou a combinação de imagens complementares, e aumentou a incerteza relacionada com as informações que os participantes desonestos possuem sobre a vítima. O aumento da expansão dos pixels incorporou informações adicionais, com a definição aleatória para autenticação ou construção dos blocos, e também forneceu o suporte de segurança ao ataque definido por LIU, WU e LIN (2011) contra o esquema HT.

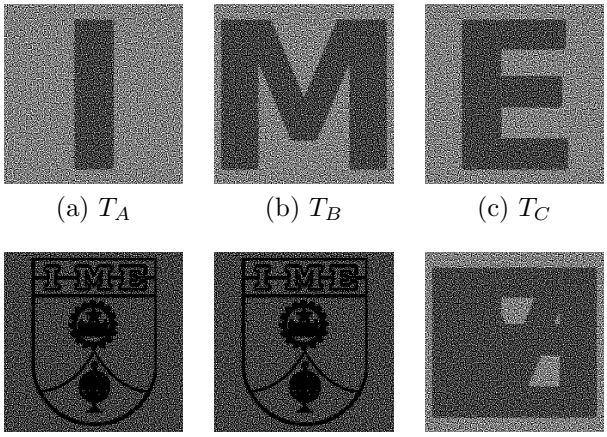
No esquema de prevenção contra fraude desenvolvido neste trabalho, foi definido que os participantes devem receber as transparências originais e as transparências circulares extras de verificação. Também foi definido que cada transparência original deve ser construída por uma versão adaptada de um $(2, n)VCS$, através da adição de m subpixels em cada matriz S_0 e S_1, de forma que cada pixel da imagem original seja expandido em $2m$ subpixels. Cada transparência circular de verificação deve ser utilizada para verificar a integridade das transparências dos outros participantes.

Conforme foi apresentado e demonstrado nos capítulos anteriores, cada participante deve enviar ao esquema, através de canais seguros, uma coleção $n^2 - n$ imagens de verificação para serem autenticadas durante a verificação da integridade das transparências dos outros participantes. Foi definido que cada imagem de verificação deve possuir alguns pré-requisitos relacionados com a segurança do esquema e por isso deve ser submetida a um processo de validação. Cada transparência circular de verificação é dividida em $n^3 - n^2$ regiões. A sobreposição entre a transparência circular de verificação de um participante com a transparência original de outro deve reconstruir em cada região, uma imagem de verificação da coleção escolhida pelo participante que realiza a verificação.

Foi definido, através de experimentos que demonstraram possíveis ataques ao novo esquema de prevenção baseado no $(2, 3)VCS$, que o percentual médio de pixels pretos contidos em cada imagem de verificação informada pelos participantes deve ser de aproximadamente 35%, no caso específico realizado no experimento em que a imagem secreta é formada pelo logo do IME. Este percentual de pixels pretos admitidos nas imagens de verificação deve ser ajustado de acordo com a imagem secreta escolhida. Torna-se necessário realizar o mesmo experimento com um banco de imagens com o objetivo de especificar um valor ideal para este limite.

É necessário realizar este experimento no novo esquema de prevenção com base em outras estruturas de acesso, como $(2, n > 3)VCS$, pois uma quantidade superior de participantes, além de Alice, Bob e Carol, pode influenciar os resultados obtidos em todos os ataques realizados neste trabalho, mais especificamente no ataque demonstrado na Seção 6.2. Também é necessário expandir o suporte aos aspectos de segurança no esquema desenvolvido neste trabalho, de um $(2, n)VCS$ para um $(k, n)VCS$. Para tornar o esquema mais abrangente, além desta expansão, a proteção deve abranger outras estruturas de acesso, como as fornecidas por ATENIESE et al. (1996a); ATENIESE et al. (1996b); ATENIESE et al. (2001).

O conceito de estrutura de acesso introduzido por ATENIESE et al. (1996a) e ATENIESE et al. (1996b), que define os subconjuntos do sistema capazes de recuperar a imagem secreta, foi desenvolvido pelos mesmos pesquisadores ATENIESE et al. (2001), e resultou no $EVCS$[5]. Neste esquema, as imagens impressas nas transparências fornecidas aos participantes em uma estrutura de acesso são formadas por imagens que podem ser identificadas pelo sistema visual deles. Ao contrário dos outros esquemas, cujas transparências são compostas por pixels aleatórios, os participantes são capazes de identificar suas imagens nas transparências após a codificação delas. Um ponto de partida para a pesquisa sobre fraude no $EVCS$ pode ser encontrado em HU e TZENG (2007). O resultado de um experimento que demonstra o $EVCS$ é apresentado na FIG. 7.1.



(a) T_A (b) T_B (c) T_C

(d) $T_A + T_B$ (e) $T_A + T_C$ (f) $T_B + T_C$

FIG. 7.1: Demonstração de $T_A + T_B = IS$, $T_A + T_C = IS$ e $T_A + T_C \neq IS$ no $EVCS$.

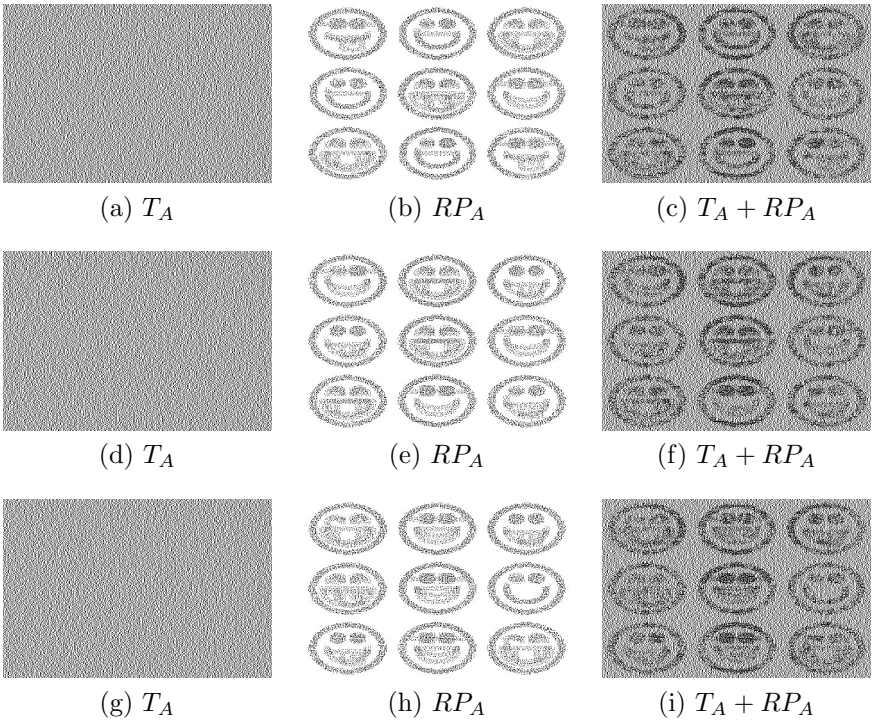
Na FIG. 7.1, foi definido o logo do IME com 150×150 pixels, para ser a IS. Alice, Bob e Carol fazem parte de uma estrutura de acesso $EA = P_A, P_B, P_C$, onde os subconjuntos qualificados são $Q = A, B, A, C$. Desta forma, somente as sobreposições $T_A + T_B$ e $T_A + T_C$ devem reconstruir IS. A sobreposição $T_B + T_C$ não deve reconstruir IS.

Alice, Bob e Carol escolheram imagens de autenticação compostas pelas letras I, M e E, respectivamente. As três transparências T_A, T_B e T_C, que podem ser visualizadas nos itens (a), (b) e (c), respectivamente, foram construídas a partir de IS com base no $EVCS$. Cada T_i possui 300×300 pixels. É possível identificar as imagens definidas pelos participantes em suas transparências. As sobreposições $T_A + T_B$, $T_A + T_C$ e $T_B + T_C$ podem ser visualizadas nos itens (d), (e) e (f), respectivamente. As sobreposições $T_A + T_B$

[5]Extended Visual Cryptography Scheme

e T_A+T_C definem a reconstrução de IS. A sobreposição T_B+T_C não define a reconstrução de IS. A estrutura de um $EVCS$ é mais complexa que a construção de um $(2,n)VCS$ e HU e TZENG (2007) definiram uma forma de realizar fraude neste esquema. É necessário realizar um novo estudo sobre a fraude e sobre possíveis esquemas de prevenção que podem ser aplicados sobre um $EVCS$.

Outra pesquisa que pode ser realizada sobre este trabalho está relacionada com a adição de uma nova métrica no módulo de validação. Esta nova métrica foi definida por SHANNON (1948) como entropia, que representa a quantidade de informação contida em uma mensagem. A entropia se opõe à parte da mensagem que é previsível e pode ser determinada. Esta métrica permitiria que o limite da quantidade de pixels pretos fosse maximizado, pois um conjunto de imagens de verificação com baixa entropia ofereceria risco menor ao ataque apresentado na Seção 6.2. É possível estabelecer uma relação entre o limite de pixels pretos e a entropia de um conjunto de imagens de verificação, com o objetivo de otimizar o suporte aos aspectos de segurança apresentados. Esta relação pode ser observada a partir de uma comparação entre os ataques da FIG. 6.9 e da FIG. 7.2.



(a) T_A (b) RP_A (c) $T_A + RP_A$

(d) T_A (e) RP_A (f) $T_A + RP_A$

(g) T_A (h) RP_A (i) $T_A + RP_A$

FIG. 7.2: Demonstração de $T_A + RP_A$ com imagens de verificação que possuem 35% de pixels pretos e baixa entropia.

O experimento foi executado três vezes, por conta de possíveis variações nos resultados do ataque, causadas pela aleatoriedade na definição do posicionamento das regiões em V_A. Foi definido o logo do IME com 150×150 pixels, para ser a IS. Na FIG. 7.2, a transparência T_A pode ser visualizada em cada execução nos itens (a), (d) e (g). Cada transparência T_A possui 300×450 pixels. A transparência RP_A, construída por Alice com base no posicionamento das imagens de verificação, pode ser visualizada nos itens (b), (e) e (h). Cada RP_A também possui 300×450 pixels. No entanto, as regiões relacionadas com as áreas com pixels brancos das imagens de verificação não são utilizadas na reconstrução.

No experimento demonstrado na FIG. 7.2, o conjunto de imagens de verificação escolhidas por Alice é formado por $i_0, ..., i_5$ da FIG. 5.3. Cada uma dessas imagens é composta por aproximadamente 35% de pixels pretos. No entanto, o resultado do experimento demonstrado na FIG. 6.9 é mais próximo da reconstrução do logo do IME, do que o resultado do experimento demonstrado na FIG. 7.2. Embora as imagens de verificação utilizadas nos dois experimentos possuam aproximadamente 35% de pixels pretos, a baixa entropia do conjunto de imagens utilizados no experimento da FIG. 7.2 e a elevada entropia no conjunto de imagens utilizados no experimento da FIG. 6.9 torna este último resultado mais interessante para Alice, embora ainda insuficiente para reconstruir a IS.

Assim como o desenvolvimento do esquema de prevenção contra fraude construído neste trabalho deve ser continuado para abranger outras estruturas de acesso, novos ataques podem ser desenvolvidos sobre ele, para que sua segurança seja fortalecida através de pesquisas relacionadas com as possíveis vulnerabilidades que possam ser encontradas, mas que não foram exploradas neste trabalho.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ATENIESE, G., BLUNDO, C., DE SANTIS, A. e STINSON, D. R. **Constructions and bounds for visual cryptography**. Em *International Colloquium on Automata, Languages and Programming*, volume 1099, págs. 416–428, Paderborn, Germany, 1996a. Springer.

ATENIESE, G., BLUNDO, C., DE SANTIS, A. e STINSON, D. R. **Visual cryptography for general access structures**. *Information and Computation*, 129(2):86–106, September 1996b.

ATENIESE, G., BLUNDO, C., DE SANTIS, A. e STINSON, D. R. **Extended capabilities for visual cryptography**. *Theoretical Computer Science*, 250(1–2):143–161, January 2001.

BLAKLEY, G. R. **Safeguarding cryptographic keys**. Em *Proceedings of the 1979 National Computer Conference*, volume 48 of *AFIPS Conference Proceedings*, págs. 313–317, New York, USA, 1979. AFIPS Press.

BLUNDO, C., D'ARCO, P., DE SANTIS, A. e STINSON, D. R. **Contrast optimal threshold visual cryptography schemes**. *SIAM Journal on Discrete Mathematics*, 16(2):224–261, 2003.

BLUNDO, C., DE SANTIS, A. e STINSON, D. R. **On the contrast in visual cryptography schemes**. *Journal of Cryptology*, 12(4):261–289, 1999.

CIMATO, S. E YANG, C.-N., editores. ***Visual Cryptography and Secret Image Sharing***. Digital Imaging and Computer Vision. CRC Press, New York, USA, 2011.

DIFFIE, W. e HELLMAN, M. E. **New directions in cryptography**. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

DIFFIE, W. e HELLMAN, M. E. **Privacy and authentication: An introduction to cryptography**. *Proceedings of the IEEE*, 67(3):397–427, March 1979.

HELLMAN, M. E. **An extension of the shannon theory approach to cryptography**. *IEEE Transactions on Information Theory*, 23(3):289–294, May 1977.

HELLMAN, M. E., DIFFIE, W. e MERKLE, R. C. **Cryptography Apparatus and Method**, 1980.

HORNG, G., CHEN, T. e TSAI, D.-S. **Cheating in visual cryptography**. *Designs, Codes and Cryptography*, 38(2):219–236, February 2006.

HSU, H.-C., CHEN, T.-S. e LIN, Y.-H. **The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing**. Em *Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control*, volume 2, págs. 996–1001, Taipei, Taiwan, 2004. IEEE Conference Publications.

HU, C.-M. e TZENG, W.-G. **Cheating prevention in visual cryptography**. *IEEE Transactions on Image Processing*, 16(1):36–45, January 2007.

KLEIN, M. ***Securing Record Communications: the TSEC/KW-26***. Center for Cryptologic History, NSA, Maryland, USA, 2003.

LIU, F., WU, C. e LIN, X. **Cheating immune visual cryptography scheme**. *IET Information Security*, 5(1):51–59, March 2011.

MENEZES, A. J., VAN OORSCHOT, P. C. e VANSTONE, S. A. ***Handbook of Applied Cryptography***. CRC Press, Florida, USA, 1 edition, October 1996.

MERKLE, R. C. **Secure communications over insecure channels**. *Communications of the ACM*, 21(4):294–299, April 1978.

NAOR, M. e PINKAS, B. **Visual authentication and identification**. Em *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, págs. 322–336, California, USA, 1997. Springer.

NAOR, M. e SHAMIR, A. **Visual cryptography**. Em *Advances in Cryptology – EuroCrypt '94*, volume 950 of *Lecture Notes in Computer Science*, págs. 1–12, Perugia, Italy, 1995. Springer.

NAOR, M. e SHAMIR, A. **Visual cryptography II: Improving the contrast via the cover base**. Em *Security Protocols Workshop*, volume 1189 of *Lecture Notes in Computer Science*, págs. 197–202, Cambridge, United Kingdom, 1996. Springer.

PRISCO, R. e SANTIS, A. **Cheating immune (2,n)-threshold visual secret sharing**. Em *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Computer Science*, págs. 216–228, Maiori, Italy, 2006. Springer.

RIVEST, R. L., SHAMIR, A. e ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. *Communications of the ACM*, 21(2): 120–126, February 1978.

SHAMIR, A. **How to share a secret**. *Communications of the ACM*, 22:612–613, November 1979.

SHANNON, C. E. **A mathematical theory of communication**. *Bell System Technical Journal*, 27:379–423, July 1948.

SHANNON, C. E. **Communication theory of secrecy systems**. *Bell Systems Technical Journal*, 28:656–715, October 1949.

SHYU, S. J., HUANG, S.-Y., LEE, Y.-K., WANG, R.-Z. e CHEN, K. **Sharing multiple secrets in visual cryptography**. *Pattern Recognition*, 40(12):3633–3651, December 2007.

STALLINGS, W. ***Cryptography and Network Security: Principles and Practice***. Prentice Hall, New Jersey, USA, 4 edition, November 2005.

STINSON, D. **Visual cryptography and threshold schemes**. *Potentials, IEEE*, 18 (1):13–16, February/March 1999.

TOMPA, M. e WOLL, H. **How to share a secret with cheaters**. *Journal of Cryptology*, 1:133–138, August 1989.

TSAI, D.-S., CHEN, T.-H. e HORNG, G. **A cheating prevention scheme for binary visual cryptography with homogeneous secret images**. *Pattern Recognition*, 40 (8):2356–2366, 2007.

VERNAM, G. S. **Secret Signaling System**, 1919.

VERNAM, G. S. **Cipher printing telegraph systems for secret wire and radio telegraphic communications**. *Transactions of the American Institute of Electrical Engineers*, 45:295–301, 1926.

WU, C. C. e CHEN, L. H. **A study on visual cryptography**. Dissertação de Mestrado, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.