Visual Cryptography for Biometric Privacy

R AVANEESH

NATIONAL INSTITUTE OF TECHNOLOGY CALICUT
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Cryptography Project
November 25, 2022

Overview of the Presentation

Objective

– Suppose a confidential location of a company requires fingerprint authentication for access.
– One method:
  – Store fingerprint directly on the company database.
  – Disadvantages:
    Even encrypted fingerprints can be leaked.
    Lightweight scanners might not be able to handle decryption schemes with high computational requirement.
– Better method:
  – Create a system which ensures that a proper fingerprint cannot be decoded even if the data stored in the database was compromised.
  – At the same time ensuring a low computational power requirement for decryption.
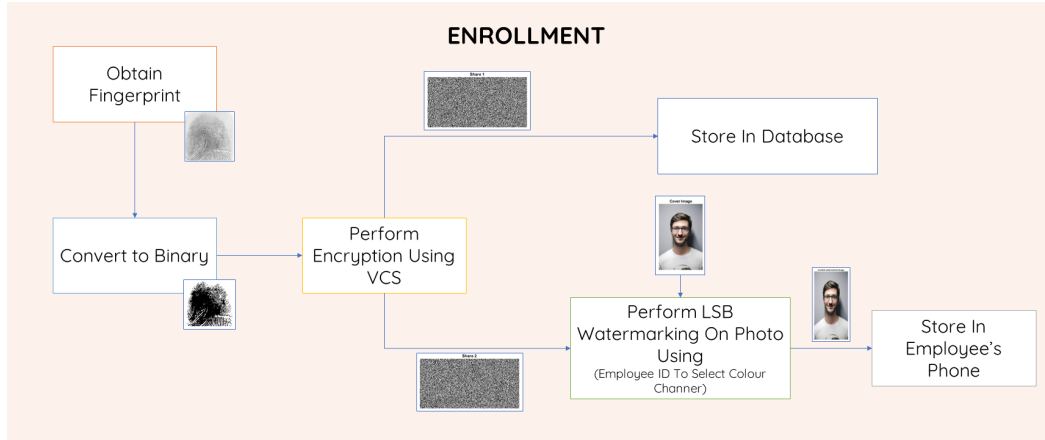
Enrollment

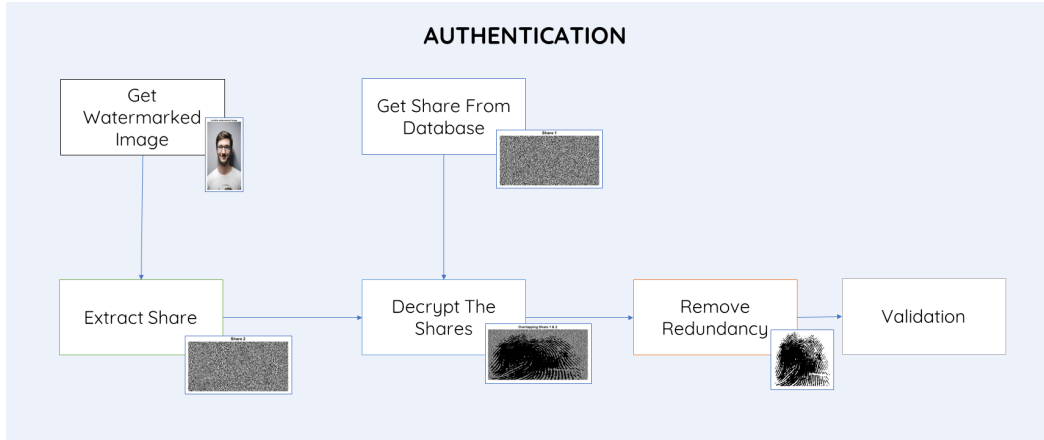Figure: Enrollment

Authentication

Figure: Authentication

Why VCS

- Decryption is simple and does not involve any cryptographic computations.
- Encryption is simple to perform and does not take much time or computational resources.
- It possesses cipher text indistinguishability as the same message is not always mapped to the exact cipher text, i.e. it is semantically secure. This is because it is probabilistic in nature.
- It is information theoretically secure.It is a visual way of secret sharing.

---

[1] *Y. Liang, H. V. Poor, S. Shamai, et al., "Information theoretic security," Foundations and Trends® in Communications and Information Theory, vol. 5, no. 4–5, pp. 355–580, 2009*

[2] *M. Naor and A. Shamir, "Visual cryptography," in Workshop on the Theory and Application of Cryptographic Techniques, pp. 1–12, Springer, 1994.*

LSB Watermarking

- LSB Watermarking, is a means for concealing an image("Secret image") in another image("cover image").
- It hides the binary secret image into the least significant bit of the cover image.
- It is easy to implement and has high fidelity.
- The impact of watermarking is negligible on the cover image.

---

[3] M. G. Almutiri and M. T. B. Othman, "Digital image watermarking based on lsb techniques: A comparative study," International Journal of Computer Applications, vol. 975, p. 8887

[4] A. Mohanarathinam, S. Kamalraj, G. Prasanna Venkatesan, R. V. Ravi, and C. Manikandababu, "Digital watermarking techniques for image security: a review," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 8, pp. 3221–3229, 2020

VCS Encryption

1. Select Secret image
2. In binary images as 0 is black and 1 white, Let the subpixels be represented as two row vectors
   - s1a = [1 0] and s1b= [1 0] for white pixel
   - s0a = [1 0] and s0b= [0 1] for black pixel
3. Generate the shares
   - For each pixel of input:
     - Choose 0 or 1 randomly (p = $\frac{1}{2}$)
     - if 0 is chosen Shares are based on subpixels given above
     - Else if 1 is chosen, new subpixels are [0 1] [0 1] for white and [0 1] [1 0] for black.
     - Store s1a/s0a in share 1 and s1b/s0b in share 2.
4. The two share have now been generated

VCS Decryption

1. Perfrom bitwise 'or' operation on share 1 and share 2
2. Negate the output
3. Remove redundancy
   - For every two pixels in recovered image, take the one with maximum value to obtain original image back
4. The image is now decrypted

LSB Watermarking - Embedding

1. Read the cover image
2. Read the watermark image to hide in the cover image
3. Determine the size of cover image and the size of watermark
4. For each row of the watermark
   - By means of RNG generate a random number 0 or 1.
   - If 1 is generated, flip the row of watermark.
5. Set the LSB of each pixel of cover image to the value of the pixels of modified watermark.
6. Generate the watermarked image.

LSB Watermarking- Extraction

1. Read in watermarked image
2. Determine the size of watermarked image
3. Use LSB of watermarked image to recover the modified watermark.
4. For each row of modified watermark
   - Using the same seed used for embedding, generate random numbers 0 or 1 by means of RNG.
   - If 1 is generated, flip the row of modified watermark.
5. Scale and display recovered watermark
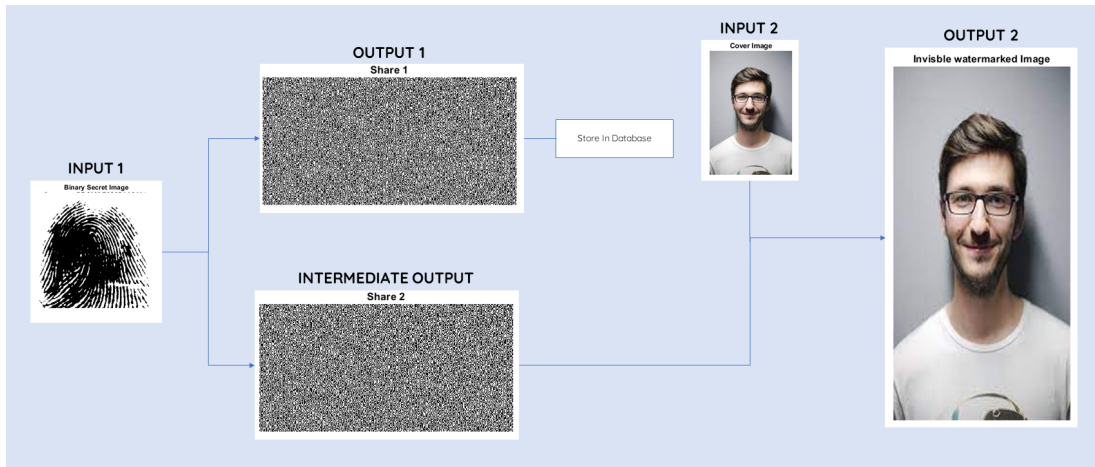
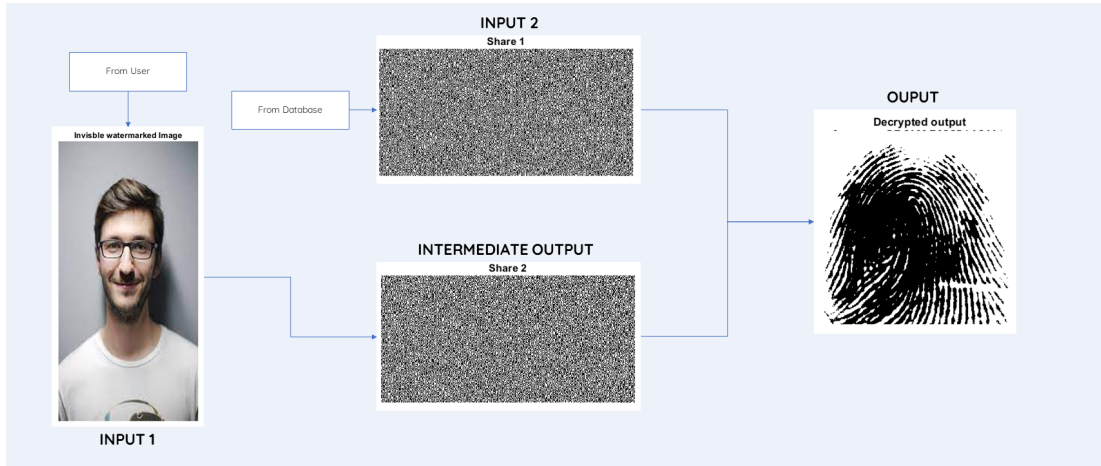# Encryption Results

Figure: Encryption

Decryption Results

Figure: Decryption

Probabilistic Nature of VCS
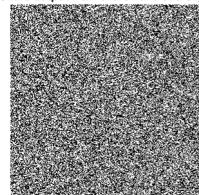
Figure: Probabilistic Nature of VCS

Comparison of Time Taken

Time take for LSB 1 Encryption
0.9301

Encryption LSB1

Time take for LSB 2 Encryption
0.9132

Encryption LSB2

Time taken for Random FLip - Encryption
1.3796

Encryption randomly LSB1 or LSB2

Time taken for Decryption
0.1651

Decryption LSB1

Time taken for Decryption
0.1787

Decryption LSB2

Time taken for Decryption
0.2437

Decryption randomly LSB1 or LSB2

Figure: Comparison of Time Taken

Analysis

LSB Watermarking

– Offers no cryptographic security.
– Offers steganographic security by hiding the presence of the second share.
– Embedding and extracting the secret share is very easy.

VCS

– It is information theoretically secure.
– Having less than 2 shares is the same as having no shares at all.
– Any share cannot be derived from any of the other shares.
– Attacker can only blindly guess the values of the shares.

Conclusion

We have implemented a system for providing access control doors by means of fingerprint authentication wherein the fingerprint data is securely stored and shared between the authenticating device and the user by means of visual cryptography and LSB watermarking.

Refrences I

📄 M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 1–12, Springer, 1994.

📄 Y. Liang, H. V. Poor, S. Shamai, *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

📄 M. G. Almutiri and M. T. B. Othman, "Digital image watermarking based on lsb techniques: A comparative study," *International Journal of Computer Applications*, vol. 975, p. 8887.

📄 A. Mohanarathinam, S. Kamalraj, G. Prasanna Venkatesan, R. V. Ravi, and C. Manikandababu, "Digital watermarking techniques for image security: a review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3221–3229, 2020.

The End