Poster Presentation On "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications"

Snehal Shantaram Patil

Indian Institute of Information Technology, Nagpur

Abstract

Core banking services encompass a range of offerings delivered through a network of interconnected bank branches. This network enables bank customers to access their accounts and execute basic financial transactions from any of the participating branch offices. One of the primary challenges in core banking is ensuring the authenticity of the customer, given the persistent threat of data breaches and hacking in the online realm. To address this authentication issue, we propose an innovative algorithm founded on image processing and visual cryptography.This poster introduces a novel technique for processing a customer's signature and subsequently dividing it into multiple shares. The total number of shares to be generated is determined by the bank's chosen scheme. When two shares are created, one is securely stored in the bank's database, while the other is retained by the customer. The customer is required to present their share during all transactions. To obtain the original signature, the customer's share is combined with the bank's stored share. The Correlation method is employed to make a decision regarding the acceptance or rejection of the output, ultimately authenticating the customer.

Introduction

In a core banking system, the risk of encountering forged signatures during transactions is a concern. Similarly, in the context of online banking, customer passwords can be vulnerable to hacking and misuse.To address these security concerns, we introduce a technique aimed at safeguarding customer information and mitigating the risks of signature forgery and password hacking.This approach leverages the principles of image processing and an enhanced form of visual cryptography. Image processing involves the manipulation of an input image to yield an output that can be an improved version of the original image or extract specific characteristics from the input image.In their work, Naor and Shamir [5] presented a straightforward yet completely secure approach for secret sharing, which requires no cryptographic computations. This method is known as the Visual Cryptography Scheme (VCS).

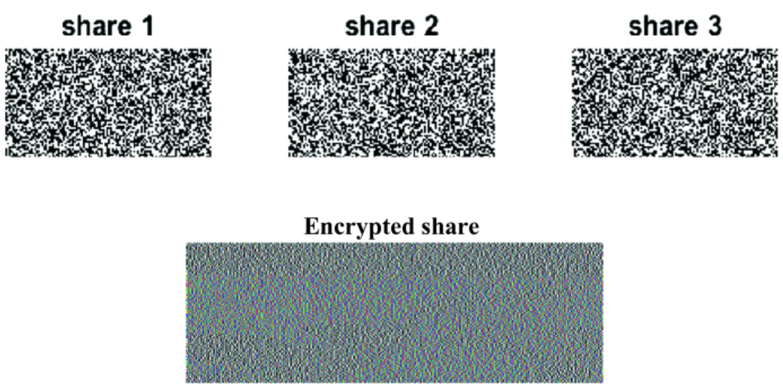
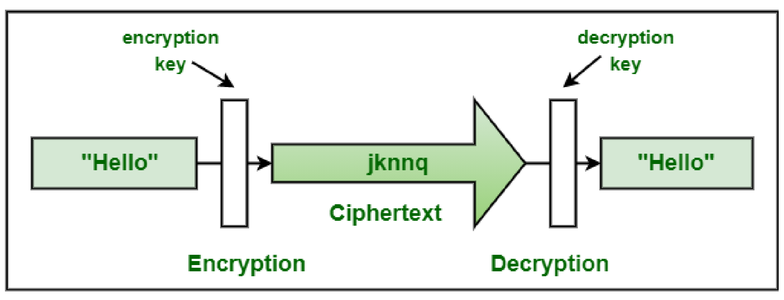


Figure 1. Visual Cryptography Scheme

The fundamental concept involves the transformation of written material into an image and subsequently encoding this image into n shadow images. The decoding process is simplified, as it only necessitates the selection of a specific subset from these n images. To reveal the hidden information, these selected images are turned into transparencies and overlaid or stacked on top of each other.



The most basic Visual Cryptography Scheme can be described as follows: A secret image comprises an array of black and white pixels, with each pixel being treated as an independent element. To encode this secret image, it is divided into n altered versions, referred to as "shares," in such a way that each pixel in a share is further subdivided into n black and white sub-pixels.
Visual cryptography schemes, first introduced by Shamir[6] and Blakley[1], aimed to safeguard cryptographic keys and found diverse applications, including access control, bank vault access, and missile launches. Borchert's segment-based approach[2] encrypts messages with symbols, such as bank account numbers, while Wei-Qi Yan's[7] VCS is tailored for printed text and images. However, Monoth's[4] recursive method is computationally complex due to sub-share encoding, and Kim's technique[3], though pixel-dithering-free, is also computationally intensive.

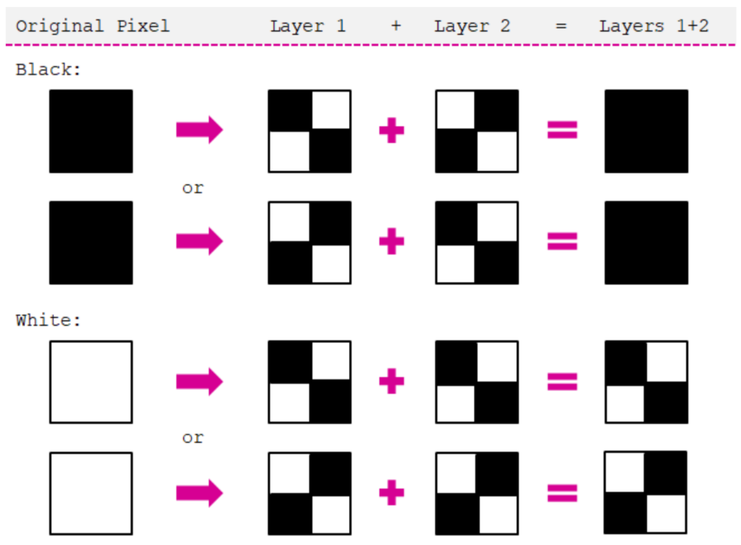
Modelling

The model for creating shares is as follows. Let P = 1, ..., n be a set of elements called participants, and let 2^P denote the set of all subsets of P. Let $\Gamma_{Qual} \subseteq 2^P$ and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \varnothing$. We refer to the members of ΓQual as qualified sets and the members of ΓForb as forbidden sets. The pair ΓQual, ΓForb) is called as access structure of the scheme.

Architechture

The architecture has the following steps:

- Pre-Processing
- Creation of Shares
- Stacking
- Post-processing
- Authentication Testing



ALGORITHM

Table 1. Algorithm

Algorithm : Creation of Shares for 2 out of 2 Scheme

Step 1: Create two matrices S0 and S1 for white and black pixels.
Step 2: Initialize two variables WHITEPIXEL and BLACKPIXEL.
Step 3: for i = 1 to rows
for j = 1 to columns
for k = 0 to 3
if Img (i, j)==WHITEPIXEL
set Share1 (i, j + k)=WHITEPIXEL
set Share2 (i, j + k)=WHITEPIXEL
else
set Share1 (i, j + k)=BLACKPIXEL
set Share2 (i, j + k)=BLACKPIXEL
end if
end for
end for
end for

Table 2. Algorithm

Algorithm : Calculate Correlation Coefficient

//Input: The original image X and the resulting image Y .
//Output: The Correlation Coefficient between X and Y .
begin
Intialize SumX = 0, SumY = 0, SumSqX = 0, SumSqY = 0 and SumXY = 0
for i = 1 to rows
for j = 1 to columns
set SumX = SumX + X (i, j)
set SumY = SumY + Y (i, j)
set SumSqX = SumSqX + $X(i,j)^2$
set SumSqY = SumSqY + $Y(i,j^2$
set SumXY = SumXY + X (i, j) ? Y (i, j)
end for
end for
AvgX = SumX/(rows ? cols)
AvgY = SumY/(rows ? cols)
EXY = SumXY/(rows ? cols)
StdX = sqrt(SumSqX/(row ? cols)$AvgX^2$)
StdY = sqrt(SumSqY/(row ? cols)$AvgY2$)
Corr = (EXY AvgX ? AvgY)/(StdX ? StdY)
end

Important Point

Scan QR code for Research Paper

IMPLEMENTATION AND PERFORMANCE ANALYSIS

- The implementation of pre-processing, post-processing and authentication testing using correlation method is done using Matlab 7. Creation of shares and stacking of shares are implemented in Java (Jdk1.5).
- . It is observed through simulation that both original image and the output image for test signatures are related with very high degree of correlation.

Simulation Results

The value of correlation coefficient may range from −1 to +1. If the value of correlation coefficient is −1, the variables X and Y are inversely related. If the value is 0, then the variables are independent and if the value is 1, then the variables are completely (or positively or directly) related.
Thus, the high degree of positive correlation indicates that the values of variables are very much close to each other.
So, if the correlation coefficient between the original image and the output image is nearer to +1, authenticity may be granted. If the correlation coefficient is nearer to zero, one can decide that the share produced by customer is fake and can be rejected.

Table 3. Generated by Spread-LaTeX

Test Images	Correlation Coefficient
Signature1	0.9089
Signature2	0.9123
Signature3	0.854
Signature4	0.9782

Conclusions

- Our proposed method enhances security in core and net banking applications by pre-processing the customer's signature, creating two shares. One share is stored in the bank's database, while the other is given to the customer for future transactions. The submitted share is matched with the bank's share, and authentication is determined using correlation techniques.
- Experimental results reveal that genuine shares exhibit a high positive correlation, validating authenticity, while fake shares exhibit no correlation. Future work could explore extending this method to color images and enhancing the quality of the decrypted image. Additionally, this approach is not limited to signatures and can be applied to any image accepted by both the bank and the customer.

Acknowledgments

I am profoundly grateful to Dr. Tapan Jain and extend my heartfelt appreciation to all the esteemed members of the ECE department at IIIT Nagpur.

References

[1] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of AFIPS Conference*, volume 48, pages 313–317, 1970.

[2] B. Borchert. Segment based visual cryptography. *WSI Press,Germany*, 69(4):320–327, 2007.

[3] S. J. Choi H. J. Kim, V. Sachnev and S. Xiang. An innocuous visual cryptography scheme. In *in Proceedings of IEEE-8 th International Workshop on Image Analysis for Multimedia Interactive Services, 2007*. IEEE, 2007.

[4] T. Monoth and A. P. Babu. Recursive visual cryptography using random basis column pixel expansion. In *in Proceedings of IEEE International Conference on Information Technology, 2007*, pages 41–43. IEEE, 2007.

[5] M. Naor and A. Shamir. Advances in cryptography -eurocrypt'94,. *Lecture Notes in Computer Science*, 950:1–12, 1995.

[6] A. Shamir. *How to Share a Secret*, volume 22. 1979.

[7] D. Jin W-Q Yan and M. S. Kanakanahalli. Visual cryptography for print and scan applications. In *IEEE Transactions, ISCAS-2004*, pages 572–575, 2004.