Design and Development of Transparent Key Authentication Protocol

Krati vyas[1], B.L.Pal[2] Prashant Joshi[3]

M.tech student, Department of C.S.E, Mewar university, Chittorgarh, India [1]

Asst.Professor, Department of C.S.E ,Mewar University, Chittorgarh, India [2]

***Abstract*- Visual cryptography is a cryptographic technique which allows visual information (Image, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an untrusted communication channel. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography. In this paper I have proposed a novel approach for authentication using visual cryptographic solutions. The protocol suggested in this paper operates on binary or binarized inputs. Therefore, natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. Then, the halftone version of the input image is used instead of the original secret image to produce the shares. The decrypted image is obtained by stacking the shares together. Because binary data can be displayed either as frosted or transparent when printed on transparencies or viewed on the screen, overlapping shares that contain seemingly random information can reveal the secret image without additional computations or any knowledge of cryptographic keys.**

Keywords – visual cryptography, human visual system, image encryption, TKA

I. INTRODUCTION

Cryptography is the art of secret writing and may be considered almost as old as writing itself. Cryptography played a crucial role throughout the history of any society that depended on information, from the Greek Skytel and the Roman Caesar cipher, over the Vigenere cipher, electromechanical rotor machines and encryption standards, to forming the backbone of electronic infrastructures in modern life.

The First cryptographic methods are known as secret-key cryptography, based on one secret key shared between the communicating parties and used both for encryption and decryption. Already apparent from this description derives its main problem, which lies in the logistics of distributing the key securely: Prior to any secret communication, the involved parties must be in possession of the same secret key [1, 2]. Nevertheless, secret-key cryptography was in use for thousands of years, adjusting its complexity to ever-increasing developments in technique and technology. Public-key cryptography was the technological revolution, solving the key distribution problem. The idea was independently discovered by Diffie and Hellman in [DH76] with Rivest, Shamir, and Adleman, providing the First implementation [RSA78], and slightly earlier but in secrecy, by Ellis, followed by Cocks' and Williamson's practical application (e.g. [Coc08]). Public-key cryptography is based on a pair of keys for each communicating party, namely a public key for encryption and a corresponding secret key for decryption, where it must hold that it is computationally infeasible (in polynomial time) of deriving the secret key from the public one. Then, we require a family of trapdoor one-way functions defining the encryption and decryption procedure. Informally, that means that encryption is a one-way operation, which is efficiently computable, given the public key, whereas the decryption function is hard to compute, unless the trapdoor is known, i.e. the secret key.

Thus, the public key can be published without compromising security, and hence, public-key cryptography does not suffer from key distribution problems. Due to that and to the fact that the technique additionally allows for digital signatures that are verifiable with the public key and yet unforgettable without the secret key, the concept of public-key cryptography is highly used and required in the age of the Internet and the proliferation of electronic communication systems.

New potential in cryptography emerged with quantum cryptography, starting with Wisner's groundbreaking paper, suggesting that "quantum mechanics allows us novel forms of coding without analogue [in classical physics]". His approach of conjugate coding did not only lay the foundations of the new cryptographic technique but also suggested a system for sending \two mutually exclusive messages", which is today known as the powerful primitive of oblivious transfer. It took several years (and the Caribbean sea) to establish quantum cryptography as a scientific discipline, accomplished by Bennett and Brassard, mainly by the BB84-protocol for quantum key distribution (QKD) after preceding work such as [BBBW82, BB83], culminating in the First practical realizations. An alternative QKD scheme was independently proposed by Ekert, based on a different approach using quantum entanglement. Since then, QKD was further researched, both on a theoretical and an experimental level. Today, conjugate BB84-coding also forms the basis for various more general quantum cryptographic tasks other than key distribution [6, 8].

Modern cryptography concerns, besides the secrecy and authenticity of communication, also the security of various other tasks. For instance, theoretical research in the sub-Field of cryptographic protocol theory covers

cryptographic primitives with fundamental properties for secure multi-party computation. Each primitive can be seen as a building block that implements some basic functionality [3]. Composition of such primitives within outer protocols yields applications that implement a specific task securely over a distance.

In general cases key distribution servers are used to transmit the shared key or public-private key. These key are transmitted through a secured channel. But what will happen when these key get published outside because nothing is so secure in now a days. Hence there is a requirement of some kind of new technique to send the key in secured way. In this dissertation I have proposed a novel method to transmit such information in a secured way [4, 5].

II. Related Work

Whenever we transmit the data (image) in the network, any unauthenticated person can read our data (image). In order to provide security to data (image) generally sender will encrypt the data (image) and send it the intended person and the receiver will decrypt the encrypted data (image) and uses it. In this dissertation we consider the problem of encrypting material (printed text, pictures etc.) in a perfectly secure way which can be decoded directly by the human visual system. The basic model consists of a printed page of cipher text (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key). The original clear text is revealed by placing the transparency with the key over the page with the cipher text. This basic model can be extended into a visual variant of the k out of n secret sharing problem: Given an image was broken up into n shares so that only someone with k or greater the k shares could decrypt the image, while any k - 1 share revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. The resulting structure can be described as n X m Boolean matrix S = [sij] where sij = 1 iff the jth sub pixel in the ith transparency is black. The grey level of the combined share is proportional to the Hamming weight H (V) of the "or" ed m-vector V. This grey level is interpreted by the visual system of the user as black if $H(V) \geq d$ and as white if $H(V) \leq d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. In the case of visual cryptography, decryption is done by human visual system. It is already discussed that human visual system acts as an OR function. In the case of decryption, for computer generated program; OR function can be used.

III. Proposed Algorithm

A. Introduction –

A solution to the k out of n visual secret sharing scheme consists of two collections of n*m Boolean matrices C0 and C1. To share a white pixel a dealer randomly chooses one of the matrices in C0, and to share a black pixel, the dealer randomly chooses one of the matrices in C1. The chosen matrix define the color of them sub pixel in each one of the n transparencies. The solution is considered valid if the following three conditions are met:

1. For any S in C0, the "or" V of any k of the n rows satisfies $H(V) \leq d - \alpha X m$.
2. For any S in C1, the "or" V of any k of the n rows satisfies $H(V) \geq d$.
3. For any subset {i1, i2, i3 ...iq} of (1, 2, 3 …..n) with $q < k$, the collections of q X m matrices Dt for $t \in \{0,1\}$ obtained by restricting each n X m matrix in Ct (where t=0, 1) to rows i1, i2,…..iq are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Condition 3 implies that by inspecting fewer than k shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. In most of our constructions, there is a function f such that the combined shares from $q < k$ transparencies consist of all the Vs with H(V)=f(q) with uniform probability distribution, regardless of whether the matrix were taken from C0 or C1. Such a scheme is called uniform. The first two conditions are called contrast and the third condition is called security.

The important parameters of a scheme are:

- m, the no. of pixel in a share . This represents the loss in resolution from the original picture to the shared one. We would like m to be small as possible.
- α, the relative differences in weight between combined shares that come from a white pixel and a black pixel in the original picture. This represents the loss in contrast. We would like α to be as large as possible.
- r, the size of the collections C0 and C1 (they need not be the same size, but in all of our constructions they are). log r represents the no. of random bits needed to generate the shares and does not affect the quality of the picture.

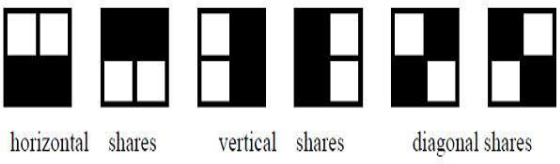

Figure 1. Shares of the image

B. Encryption-

Step I: *Take an image as input and calculate its width (w) and height (h).*

Step II: *Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image. k must be less than or equal to n.*

Step III: *Calculate recons = (n-k)+1.*

Step IV: *Create a three dimensional array img_share[n][w*h][32] to store the pixels of n number of shares.*

Step V:

*For i=0 to (w*h-1)*

{

Scan each pixel value of the image and convert it into 32 bit binary string let PIX.

For j=0 to 31

{

If ith position of PIX contains 1 call Random_Place(n, recons)

For k=0 to (recons-1)

{

Set img_share[rand[k]][i][j] = 1

}

}

}

Step VI: *Create a one dimensional array img_cons[n] to store constructed pixels of each share.*

Step VII:

For k1=0 to (n-1)

{

*For k2=0 to (w*h-1)*

{

String value=""

For k3=0 to 31

{

Value=value+img_share[k1][k2][k3]

}

Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0. Construct pixel from these part and store it into img_cons[k1].

}

Generate image from img_cons[k1].

}

Subroutine int Random_Place(n,recons)

{

Create an array rand [recons] to store the random number generated.

For i=0 to (recons-1)

{

Generate a random number within n, let rand int.

If (rand int is not in rand [recons]) rand[i] = rand int.

}

Return rand [recons]

}

C. Decryption-

Step I: *Input number of shares to be taken (k), height (h) and width (w) of each share.*

Step II: *Create a two dimensional array share[k][w*h] to store the pixel values of each share. Create a one dimensional array final [w*h] to store the final pixel values of the image to be produced by performing OR operation.*

Step III:

for i=0 to k-1

{

Input the name of the ith image share to be taken.

*For j=0 to (w*h-1)*

{

Scan each pixel value of the ith image share and store the value in share[i][j].

}

}

Step IV:

For i=0 to (k-1)

{

*For j=0 to (w*h - 1)*

{

final [j] = final [j] — share[i][j]; [— is bitwise OR]

}

}

Step V: *Generate image from final [w*h].*

IV. RESULTS

- Generation of transparency for a text: shared_key

Figure 2. Image generation for a text "shared_key"

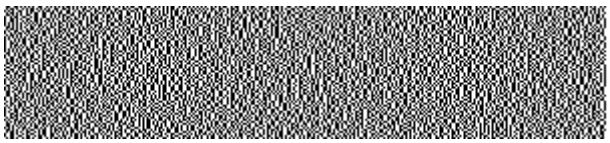

Figure 3. Share 1 for the image generated earlier

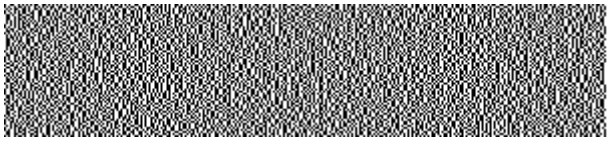

Figure 4. Share 2 for the image generated earlier

- Reconstruction of key with adding two shares received at receiver side.

Figure 5. Image obtained after combining shares at receiver side

CONCLUSION

Visual Cryptography technique helps us recovering from problems of size of the image file, Network security by reducing the file size or by compressing it and increasing the network Security by encrypting the image using algorithms which further reduces the cyber crime or hacking. We have presented a new visual cryptographic system which can be used to hide the original information from an intruder or an unwanted user.

The advantages of the proposed method are its resizing factor and its capability of reconstruction f the secret image. This work is an attempt to make a secured transfer of valuable images between two trusted parties

REFERENCE

[1] N. Alon, O. Goldreich, J. Hastad and R. Peralta, "Simple constructions of almost k-wise independent random variables Random Structures and Algorithms", Vol. 3, pp. 289-304, 1992.

[2] N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth, "Construction of asymptotically good low-rate error-correcting codes through pseudorandom graphs", IEEE Transactions on Information Theory, pp. 509-516, 1992.

[3] Evgeny Milanov, "The RSA Algorithm", Washington University, 2009

[4] F. J. MacWilliams and N. J. A. Sloane, "The theory of error correcting codes", North Holland, Amsterdam, 1977.

[5] J. L. Carter and M. N. Wegman, "Universal classes of hash functions", Journal of Computer and System Sciences", pp. 143-154, 1979.

[6] Amit Dhir, "Data Encryption using DES/Triple-DESFunctionality in Spartan-II FPGAs", Whit Paper, WP115 (V. 1.0), 2000.

[7] N Alon and J Spencer, "The probabilistic method", Wiley, 1992.

[8] J. Kahn, N. Linial and A. Samorodnitsky, "Inclusionexlusion exact and approximate", manuscript

[9] N. Linial and N. Nisan, "Approximate inclusionexlusion", Combinatorica, pp. 349-365, 1990.

[10] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality", Journal of Computer and System Sciences, pp. 265-279, 1981