

A Novel Key Distribution Scheme for a Visual Crypto System

Kalyan Das¹, Aromita Sen²

¹Department of Information Technology, St. Thomas College of Engineering and Technology, Kolkata, India

²Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology Kolkata

Abstract - With the high speed advancement of Computer network and internet, has hiked the chance of data snooped during the time of transmission. In this issue, Cryptography plays a vital role, which hides the actual information using some secret key and thereby converts it into an alternative equivalent multimedia file like image, video or audio in such a way that only the intended recipient can retrieve back the original data. Here in this paper, a novel secret sharing technique has been suggested, which comprises of two main parts. The first part for establishing shared secret key (one time key), using asymmetric key cryptography and then transmit the confidential data using that shared secret key, ensuring the confidentiality and integrity. Here for the encoding purpose Modulus Operation is used to increase the difficulty for the inverse function.

Key Words: Visual Cryptography, Encryption, Decryption, Key Distribution, Pixel, Data Security, Cryptanalysis

1. INTRODUCTION

Cryptography is a Greek word. It literally means hidden writing it's the science and the art of making secret codes. Encryption is the process of taking a message transforming it by replacing letters and changing it around until it looks like something totally not like a message that nobody can read you can send it to your destination and then they can decrypt it and get back the original data or the message that was there. Until a few decades ago, the information was collected by an organization and stored on physical files. But now, information storage become electronic and thus implementation of their confidentiality, integrity and availability become more different and challenging.

To deal with all those security issues, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography requiring less computation and less storage. Cryptography, a word with Greek origin, means "secret writing". It refers to encryption and decryption of secret messages using secret keys.

VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

• (2, 2) Threshold VCS scheme- This is the simplest threshold scheme that encrypts a secret message in two different

shares such that it reveals the secret image when they are overlaid.

• (n, n) Threshold VCS scheme- In this scheme the secret message is encrypted into n shares, such that when all of the n shares are combined, it will reveal the secret message.

• (k, n) Threshold VCS scheme- This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

The question on key exchange was one of the first problems addressed by a cryptographic protocol that was prior to the invention of Public Key Cryptography. In case of Symmetric Key Cryptography, the point is to agree on a key that two parties can use for encryption, in such a way that the eavesdropper cannot attain the key.

Our prime objective is to suggest a strong protected transmission technique which ensures secure potential message transmission, from one end to another over a local area network, using image processing based cryptography techniques.

1.1 Preliminaries

•Cryptography: Cryptography is the study and practice of protecting information by data encoding and transformation techniques. The primary goal of cryptography is to conceal data to protect it against unauthorized third-party access by applying encryption. The more theoretical or mathematical effort is required for an unauthorized third party to recover data, the stronger is the encryption.

•Encryption: In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

•Cipher: An encrypted message is known as cipher text.

•Decryption: Decryption is the inverse of encryption; the process of taking cipher text (encrypted data) and a cryptographic key, and producing clear text (the original non-encrypted data)

•Symmetric Key Cryptography: It is also referred to by another term like: Secret Key Cryptography. In this scheme, only one key is used and the same key is used for both encryption and decryption of messages. Obviously, both the

parties must agree upon the key before any transmission begins and nobody else should know about it.

Basically, at the sender's end the key transforms the plain text message into cipher text form. At the receiver's end, the same key is used to decrypt the encrypted message, thus retrieving the original message out of it. Example: DES (Data Encryption Standard)

•Asymmetric Key Cryptography: In Asymmetric Key Cryptography, also called as Public Key Cryptography, two different keys (which form a key pair) are used. One key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message – not even the original (i.e. the first) key can be used for encryption.

•Pixel: In digital imaging, a pixel, or picture element is a physical point in a raster image, or the smallest addressable element in a display device. The address of a pixel corresponds to its physical coordinates. Each pixel is a sample of an original image; more samples typically provide more accurate representations of the original. The intensity of each pixel is variable. In color image systems, a color is typically represented by three or four component intensities such as red, green, and blue, or cyan, magenta, yellow, and black.

•Modular Arithmetic: The division relationship $(a = q \cdot n + r)$ has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we only deal with the remainder r. We don't care about the quotient. The modulo operator (mod) takes an integer (a) from the set Z and a positive modulus (n). The operator creates r that is $a \text{ mod } n = r$

2. EXISTING WORK

Diffie-Hellman Key Exchange Algorithm

Suppose two participants Alice and Bob are allowed to communicate over a line which is tapped. So any message they pass can be intercepted and misused by Eve, who is always listening to that channel. The trick is to agree on a secret numerical key without the knowledge of the intruder.. This trick is done using colors so how could Alice & Bob agree on a secret color without Eve finding it out. The key agreement protocol named as Diffie-Hellman Key Exchange Algorithm(1976)[2] was the first method for establishing a shared secret over an unsecured communication channel.

The trick is based on two facts. One it's easy to mix two colors together to make a third color and to give it a mixed color, but it's hard to reverse it in order to find the exact original colors. This is the basis for a lock is easy in one direction and hard in the reverse direction. This is known as a one-way function.

First they publicly agree on a starting color say yellow. Next Alice and Bob randomly select their own private colors and mix them into the public yellow in order to disguise their private color. Now both of them keeps their private color and sends the mixture to the other one. Now the heart of the trick

is, Alice and Bob add their private colors to the other person's mixture that has arrived and get the shared secret color. Now Eve is unable to determine this color since she needs one of the private colors to do so.

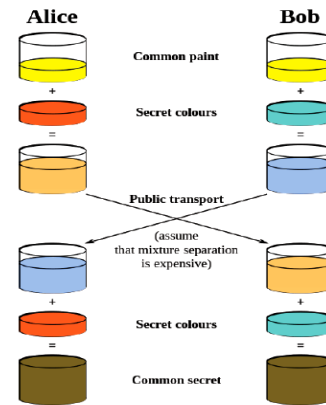


Figure1. Illustration of the Diffie–Hellman Key Exchange

Now to do the same with numbers we need a numerical procedure which is easy in one direction and hard in the reverse direction, which brings us to modular arithmetic which is known as clock arithmetic. For example to find $46 \text{ mod } 12$ we take a rope of length 46 units and wrap it around a clock of 12 units which is called the modulus and wherever the rope ends is the solution.

Now to make this work we need a prime modulus such as 17 instead of 12 then we find the primitive root of 17 which is a number that has no factors in common in this case 3 and it has this important property that when raised two different exponents the solution distributes uniformly around the clock three is known as the generator. So if we raised 3 to any exponent X the solution is equally likely to be any integer between 0 and 17. Now we have our one-way function easy to perform but hard to reverse, we have to do trial and error in order to find the matching.

The steps are as follows:

1. Alice chooses a large random integer x within the range of $0 <= x <= p-1$ and sends Bob $X = g^x \text{ mod } p$
2. Bob chooses a large random integer y within the range of $0 <= y <= q-1$ and sends Alice $Y = g^y \text{ mod } p$
3. Alice computes $k = Y^x \text{ mod } p$
4. Bob computes $k = X^y \text{ mod } p$

k is the symmetric key. k is equal to $g^{xy} \text{ mod } n$. Both have received the same value without Bob knowing the value of x and without Alice knowing the value of y.

Alice and Bob want to be able to generate a key to use for subsequent message exchange. The key generating exchange can take place over an unsecured channel that allows eavesdropping. The ingredients to the protocol are: p, a large prime and g, a primitive element of Z_n . These two numbers do not need to be confidential. They can be sent through the internet.

Exponent is easy with small numbers but if we use a prime modulus, which is hundreds of digits long, it starts to get seriously hard even if you had access to all the computational power on earth it could take thousands of years or more to find the answer. So the strength of a one-way function is based on the time needed to reverse it.

Security Analysis

The Diffie-Hellman Scheme does not provide authentication of any kind. It only allows 2 anonymous parties to share a common secret. But for all Alice knows, she could be shaking hands with the devil (instead of Bob). The eve doesn't need to find out the value of x and y to attack the protocol. She can fool Alice and Bob by creating two keys: one between herself and Alice, and another between herself and Bob. This is why we need at least one party to be authenticated. Thus the Diffie-Hellman algorithm fails to provide security over man-in-the-middle attack.

To overcome this problem, we have suggested a new technique for key transmission over public channel securely, without letting others know about it, by not sharing the information directly, but creating a key together.

3. PROPOSED METHOD

Most of the visual cryptographic scheme uses a set of values as a key or a dictionary which has been used during the substitution technique. For this it is better to use a secure technique than direct transmission of the content. That's why we have introduced a new technique for key exchange as a reflection of the Diffie-Hellman Key Exchange algorithm. One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. One solution to this problem is to hide information in digital media and use of key for further security. Here we have used cover images (colored) for the hiding part.

In proposed technique a new secret sharing technique has been suggested where we have used the concept of asymmetric key cryptography for transmitting a secret symmetric key to both the parties, which they will be using for further communication (encryption & decryption) without letting others know about their original secret keys. Here initially a key value is decided between both the parties, which need not to be confidential and known as the public key. Then both the parties Alice and Bob have decided their own secret keys which are only known to them. Then they have applied modulus operation to both their secret keys using the public key. And after that the computed values are sent over the secure network. Then both of them again need to apply some mathematical operation over the received data and their secret keys in order to generate the symmetric key which they will be using for their future communication.

The proposed scheme has been considered secured against the large number of arithmetic operations need to be performed in order to generate the key.

After some experiments over various data sets, we have found that in all the cases, both the parties are retrieving the same key, which is ready for future use. As here we are using modulus operation which is not reversible and we are not sending the secret keys directly, we are limiting the chance of eavesdropping during the transmission.

4. METHODOLOGY

In additive model or RGB model, every color image is composed of pixels where each pixel is a series of bits composed of RGB values with 24bit depth. Each value is in the range of 0-255 i.e. Red ranges from 0-255, Green ranges from 0-255 and Blue ranges from 0-255. When all these three values for RGB are combined we get a color which defines the pixel of the image.

While calculating the intensity values, if we get a value which is less than "0" i.e. negative value, we have considered those as value "0" and all other intensity values in unit8 format.

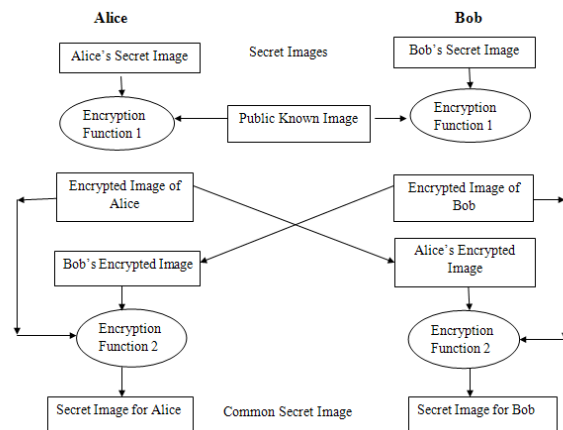


Figure2. Flow chart representation of the proposed scheme
Brief description of each step

Alice and Bob are the sender and receiver of the potential messages who need to agree on a similar key for transmission of secrets using symmetric key cryptography algorithms, in such a way that the eavesdropper can't get any knowledge about the key. As here we are using visual cryptography for the key transmission, so we have considered the key to be an image.

- Step 1: Firstly Alice and bob publicly decided a key which is a non-zero positive number and a color image which is of the same size that of the secret key.
- Step 2: Then Alice and Bob privately decided their own private keys, let them to be A and B.
- Step 3: Now they will apply the encrypt function 1 on their private keys along with the public image. Let the outputs to be A' and B' respectively.
- Step 4: Now they will exchange the keys among them.
- Step 5: Then the encrypt function 2 will be applied on their own sent data and received data, i.e. Alice will operate on A and B' & Bob will operate on B and A'.
- After the final operation they both will be holding the same key.

For the encryption functions, each time we will use the modulus operation with help of the public key.

5. IMPLEMENTATION DETAILS





















The above mentioned scheme is implemented into “MATLAB R2009a and IrfanView have been used as the basic image editing software. This technique can work for both color images as well as gray scale images. After some experiments over various data sets, we have found that in all the cases both the parties are retrieving the same key, which is ready for future use.

6. EXPERIMENTAL RESULTS

Below is a set of Output Generated for different key values and public shared image as ‘peppers.jpg’. All the images used are in 512*512*24bit size and the average elapsed time is as follows:

- Encryption 1 for Alice: Elapsed time is 0.110362 seconds.
- Encryption 1 for Bob: Elapsed time is 0.112347 seconds.
- Encryption 2 for Alice: Elapsed time is 0.007116 seconds.
- Encryption 2 for bob: Elapsed time is 0.006040 seconds.

Table 1. Resultant Output of the Proposed Scheme

Sl No	Public Key	Secret Image of Alice	Secret Image of Bob	Alice's Encrypted Image	Bob's Encrypted Image	Generated Secret image
1.	Key= 47					
2.	Key= 58					
3.	Key= 96					
4.	Key= 112					

Quality Measurement

In this process we have taken some well known benchmark images for the experimental purpose. For performance calculation we need to use SSIM or PSNR index. Here we have used the PSNR index for measuring the quality between two images. In PSNR quality measurement one of the images are compared provided the other image is regarded as of perfect quality. The formulae used are given below:

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i, j) - Y(i, j)]^2 \quad \dots\dots \text{Eq1}$$

$$PSNR = 10 \log_{10} \left(\frac{I_{max}^2}{MSE} \right) \quad \dots\dots \text{Eq2}$$

[X is the original image and Y is the output image; I is the dynamic range of pixel values normally 255; (M,N) are the dimensions of the image]

The quality measures are calculated between the original image and the encrypted images. Table2 shows the quality measures of the images after encryption process.

Table2. Experimental results for Key Generation process

Sl. No.	PSNR index for Alice's Images		PSNR index for Bob's Images	
	Encrypted Image 1	Encrypted Image 2	Encrypted Image 1	Encrypted Image 2
1	8.1683	7.2935	13.7294	12.2402
	9.1421	8.2051	12.7471	11.3551
	11.6839}	10.5477	11.0015	9.8864
2	10.8872	9.7806	13.9658	12.5978
	11.6542	10.4960	13.1101	11.7273
	12.1304	10.8304	11.3852	9.9410
3	12.1567	9.5964	16.9360	12.6188
	14.3039	11.3913	15.8081	11.9538
	15.5573	11.9212	13.0325	10.0645
4	11.5731	9.7383	14.7120	12.7470
	15.3968	13.3323	14.2854	12.2081
	16.6778	14.8573	12.6960	10.6767

7. CONCLUSIONS

We have applied the proposed method in several image sets with different values for the public key and retrieved different results. In all the cases the generated secret key is far different from the original private message which ensures the confidentiality in the scheme.

As conclusion it can be said that, the proposed key sharing scheme is undoubtedly fine and fantastic to use. In our proposed algorithm the same secret key is retrieved in both the sides. The same technique can be used on binary or gray scale images also without any change in the algorithm. Till now we haven't considered the noise included in the image during transmission and changes included due to that, but we will be checking those facts in the near future and work on that matter as per needed. This project can be extended further to implement key agreement for a group without increasing the bandwidth requirement in a secured manner.

ACKNOWLEDGEMENT

We are very grateful to all authors in reference section. Their methods, algorithms, conceptual techniques are very helpful for our research

REFERENCES

- [1] https://en.wikipedia.org/wiki/Visual_cryptography
- [2] <http://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english>
- [3] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- [4] Moni Naor and Adi Shamir, "Visual Cryptography", *advances in cryptology- Eurocrypt*, 1995, pp 1-12.
- [5] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998
- [6] H. C. Hsu, T.S.Chen, Y.H.Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 2004, pp. 996-1001.
- [7] H.-C.Wu, C.-C.Chang, "Sharing Visual Multi-Secrets Using Circle Shares", *Comput. Stand. Interfaces* 134 (28), pp.123-135,(2005).
- [8] E. Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes. " *Designs, Codes and Cryptography*, 11(2), pp.179-196, 1997.
- [9] C. Yang and C. Lai, "New Colored Visual Secret Sharing Schemes", *Designs, Codes and cryptography*, 20, 2000, pp. 325-335.
- [10] C. Chang, C. Tsai, and T. Chen., "A New Scheme For Sharing Secret Color Images In Computer Network", *Proceedings of International Conference on Parallel and Distributed Systems*, pp. 21-27, July 2000
- [11] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", *Proceedings of APCC2008, IEICE*, 2008
- [12] "Digital Image Processing Using MATLAB", 2nd Ed. by Gonzalez, Woods, and Eddins
- [13] "Digital Image Processing", 2nd Ed. by Gonzalez, Woods, and Eddins
- [14] "Cryptography and Network Security" by Atul Kahate
- [15] "Cryptography and network Security", by B.A.Forouzan and Debdeep Mukhopadhyay