A Secure Visual Cryptography using a Hybrid Technique of Vigenere Cipher, Dithering Matrix and RSA Algorithm

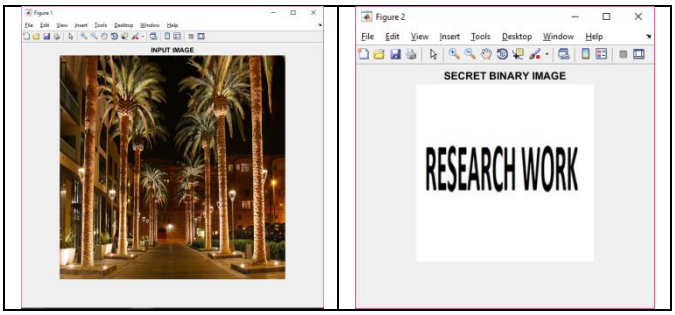
Er. Varinder Saini[1], Er. Rajandeep Kaur[2]
[1]*Computer Science and Engineering, SBBSU (Sant Baba Bhag Singh University) Jalandhar, India*
[2]*AP, Computer Science and Engineering, SBBSU (Sant Baba Bhag Singh University), Jalandhar, India*

Abstract-- Visual Cryptography is one of the reliable techniques for the security purpose. In this technique we divide the image into shares and then these shares are encrypted using encryption algorithms. It is proposed by Naor and Shamir in 1994. It is secure technique that allows sharing of secret images without any complex cryptographic computation, which they termed as Visual Cryptography. The proposed technique use vigenère cipher algorithm, RSA algorithm and dithering matrix algorithm for high security of images and secret information. Both encryption algorithms double the security while transferring images over the network. The proposed scheme also uses the concept of half toning and reverses half toning for improving the quality of a secret image.

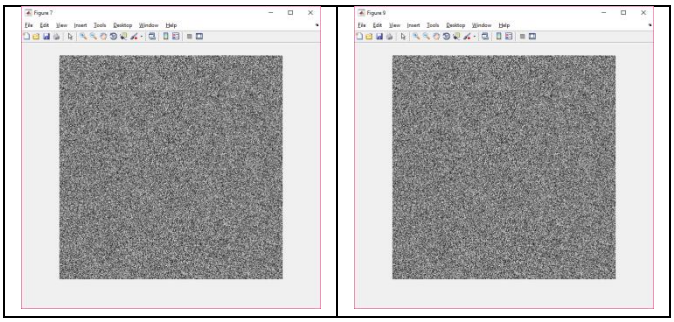
Keywords: *Cryptography, Visual Cryptography, Encryption, Vigenere cipher encryption technique, MSE, PSNR, RSA, MATLAB.*

I. INTRODUCTION

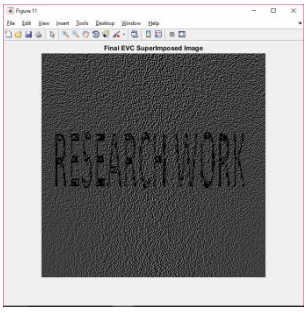
Visual cryptography is an encryption process which is used to hide information in images. It is the art of encrypting visual information such as handwritten text, images etc. The encryption takes place in such a way that no complex mathematical computations are required in order to decrypt the secret Visual Cryptography Schemes is a technique of image encryption novel to hide the secret information in images [1].Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography. It uses two or more transient images (called shares). One picture contains arbitrary pixels and the other picture contains the secret information that is hidden. It is impossible to recover the secret information from any one of the pictures i.e. images. Either transparent images or layers are required to reveal the secret information [2]. The simple method to implement visual cryptography is to print the two layers onto a transparent sheet. When any random image containing random pixels then it can be seen as one-time pad system and it will present indestructible encryption. In visual cryptography, the bit of message consists of a collection of white and black pixels i.e. it is assumed to be a binary image and each pixel is handled separately [3].



Original image Secret image



Encrypted share 1 Encrypted share 2



Final Retrieved secret image

Fig.1: Illustration of Visual Cryptography

Each original pixel appears in n modified versions called shares of the image, one for each transparency. Each share contains m black and white sub pixels. Each share of the sub pixels is printed on the transparency in close proximity [2].

II. PROPOSED TECHNIQUE

The new technique has been purposed to hide the information along with security. The main aim of this technique can be purposed for the security of the secret information. The basic idea of this process selects the cover image and then selects the secret image. Now, perform the encryption technique vigenère cipher algorithm. If entered the correct key then half toning process starts and otherwise terminate the process. Then apply dithering matrix algorithm and the halftone image is created. After this perform reverse half toning process and the reverse half toned image is created. And then secret information is hidden in share 1 and share 2. Perform Encryption and Decryption of Share -1 and Share -2 using RSA Algorithm. At the end retrieve the final secret image. After that generate results in form of PSNR and MSE. PSNR (peak signal to noise ratio) is used to check the quality of the original image and the secret image. MSE (mean square error) is used to measure the average square error between the original image and the secret image. As the purposed technique uses the vigenère cipher encryption technique and RSA encryption algorithm, thus it provides more security while using dithering matrix algorithm helps to hide the secret information. In this proposed technique, use of two RSA algorithms of public key cryptography encryption and decryption performed on share1 and share2 that provide security of shares. And vigenère cipher encryption technique used for security purpose. If the correct key entered then next process starts otherwise terminate the process. If hackers get one share, then the hacker is not able to retrieve the secret information from one of the images.

III. ANALYSIS OF RESULT

Proposed system of secure visual cryptography implemented by combining the vigenère cipher, dithering matrix algorithm and RSA algorithm for security of secret images. For achieving the goals of the proposed system MATLAB R2015a is used. The result is basically implemented with the help of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) parameters. PSNR is calculated to check the quality of an output image. Higher the value of PSNR, better the quality of an output image. But for the better results MSE value should be low. In the proposed system RSA and vigenère cipher algorithms are used for encryption. These are described below:

RSA:

RSA is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 [4]. RSA is a cryptosystem, which is also known as public key cryptosystems [5]. RSA is normally used for secure data transmission. This technique will make the information to be transmitted into an unintelligible form by encryption so that only authorized persons can correctly recover the information [6].

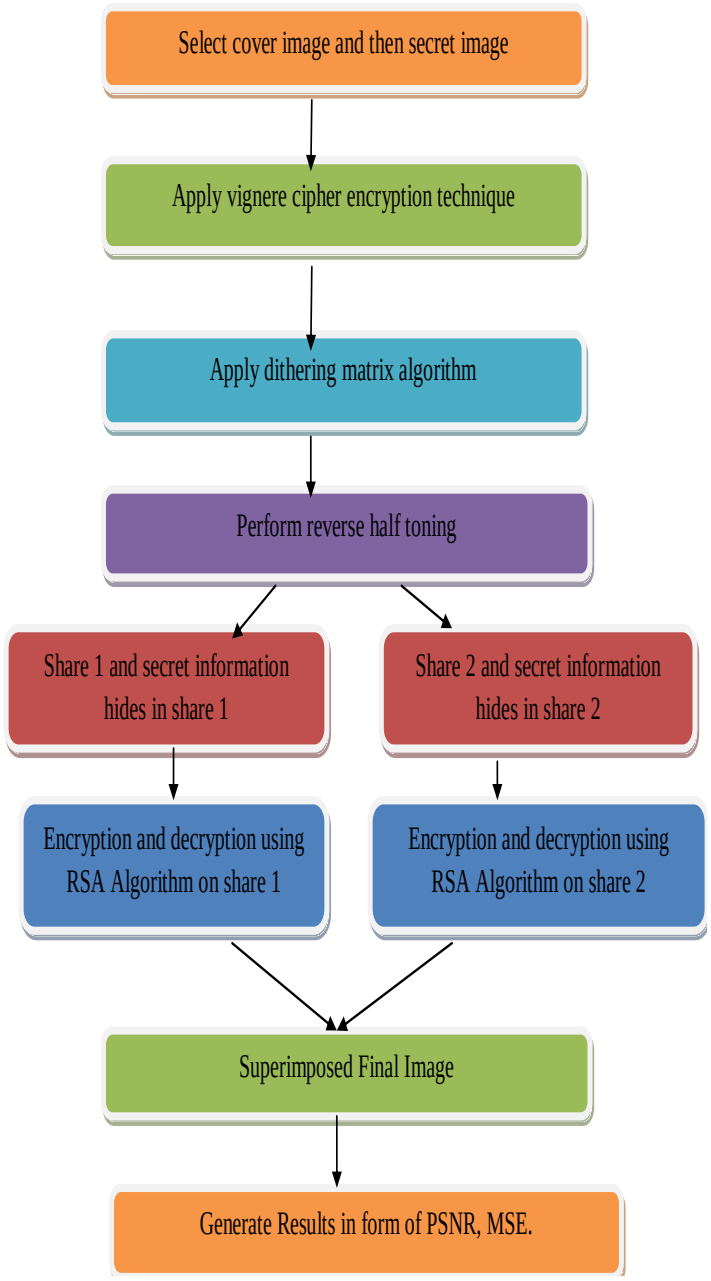


Fig.2: Proposed Technique

RSA implementation consists of three phases:

1. Key generation
2. Encryption
3. Decryption [6]

Vigenere cipher algorithm:
Vigenere cipher encryption technique is purposed by the blaise de vigenère from the court of Henry of France in the sixteen century. It uses a 26*26 table with A to Z as the row heading and column heading. It can be performed by exchanging letters with numbers.

Vigenere cipher Encryption Formula:
$C_I = (p_i + k_I) \bmod 26$

C_i is the I^{th} letter of text encoding results

P_i is the i^{th} letter of the original text

K_i is the i_{th} letter of the keyword

Vigenere Cipher Decryption formula

$C_i = p_i + k_{i)} - 26$

Vigenere cipher encryption method is used to encrypt the text that can hide inside the image. It provides more security that cannot see by the naked eyes. In proposed technique analysis is on the basis of parameters. Parameters can be used in this purposed technique are PSNR and MSE. Parameters can be described as follow:

Peak Signal to Noise Ratio
PSNR is used to measure the quality of the image after the reconstruction. Higher PSNR value shows that secret image quality is better than the original image. The peak signal-to-noise ratio (PSNR) is a ratio between maximum power of a signal and the signal's noise power. PSNR is usually expressed in decibels, which is a logarithmic scale [8].The PSNR between two images having 8 bits per pixels or samples can be described as follow:

$PSNR = 10 \log_{10} [MAX^2/MSE]$

Where, MAX^2= Maximum value of pixel in original image

MSE= Mean Square error

Mean Square Error
MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss [7]. MSE calculate the average of the squares of the "errors." Error is the amount by which the value implied by estimator different from the amount to be estimated. The difference occurs due to randomness or because the estimator does not account for an information that could construct more accurate estimate. Mean Square Error is the risk function that represents the cumulative error between the original image and the secret image [8]. It is represents as follow:

$$\mathbf{MSE= 1/MN \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(X, Y)-S(X, Y)^2}$$

Where (X, Y) are the two Coordinates of the image, (M, N) are the two dimensions. So (X, Y) creates Secret image and (C, Y) creates cover image. In MATLAB to measure the parameter PSNR and MSE use this measerr. These are approximation quality metrics.

Syntax
[PSNR, MSE] = measerr(X, XAPP)

Description
[PSNR, MSE]=measerr(X, XAPP) returns the peak signal-to-noise ratio, PSNR, mean square error, MSE, maximum squared error, and ratio of squared norms, X, and its approximation, XAPP.

TABLE 1: Comparative analysis of existing techniques RSA, LSB with proposed technique in terms of PSNR and MSE values

Picture Quality Evaluation	PSNR	MSE
RSA	8.6666	8.8394
LSB	40.9335	5.2448
Proposed technique	54.8303	0.2138

The Table 1 shows the performance of the system in terms of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error).The results show that Proposed technique shows better results in case of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Ratio) because for better results the value of PSNR is high and the value of MSE is low.

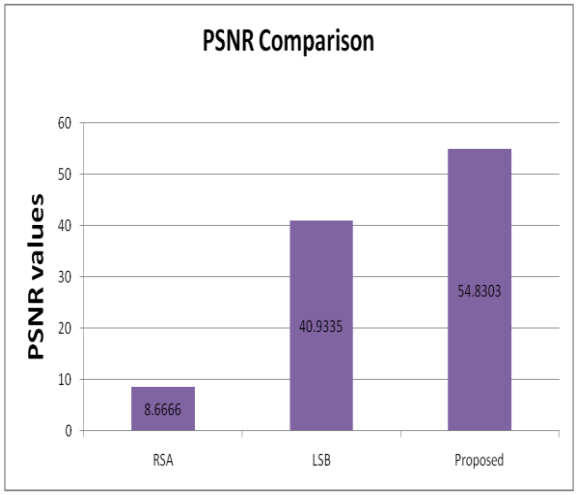


Fig.3: Comparison between MSE Values of RSA, LSB and Proposed Technique

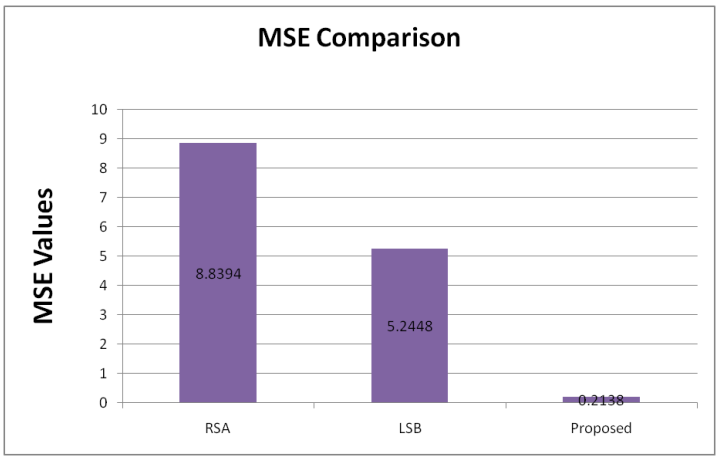


Fig.4: Comparison between MSE Values of RSA, LSB and Proposed Technique

IV. CONCLUSION AND FUTURE SCOPE

With the rapid evolution of digital media, it is becoming very important to find a method to protect the security of the images. An efficient method for securely transmitting images is Visual Cryptography. In my work proposed Visual Cryptography technique depending on some complex computations like vigenère cipher encryption technique and RSA algorithm which giving double security than the traditional methods which using only XOR operation. The proposed system works only on two dimensional images. In future, this system can be extended to work for three dimensional images. This system enhances the security by using double later encryption and dithering algorithm. In future the quality of retrieved image can also be improved.

V. REFERENCES

[1] Shruti M. Rakhunde, Manisha Gedam," Survey on Visual Cryptography: Techniques, Advantages and Applications", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 06-12.

[2] Febin Baby, Arun R, Dr. Suvanam Sasidhar Babu," ViCry: Visual Cryptography Schemes for Security (An overview of different types of visual cryptography schemes)", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 15-18.

[3] Monika Bhosale, Rajshree Chaudhary, PrathameshGaddam, AyushiKedar Yogesh. J.Pawar, "Visual Cryptography Scheme for Secret Image Retrieval", in IJARSET Vol. 3, Issue 3 March 2016.

[4] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's" in IJARCSSE, Vol. 2, Issue 7, July 2012.

[5] Shikha Kuchhal, Ishank Kuchhal," Data Security Using RSA Algorithm In Matlab" in IJIRD, July, 2013, Volume 2, Issue 7.

[6] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran," Digital Image Encryption Based on RSA Algorithm", Journal of Electronics and Communication Engineering, Volume 9, Issue 1, Jan. 2014

[7] Anshul Sharma, "PERFORMANCE OF ERROR FILTERS IN HALFTONE VISUAL CRYPTOGRAPHY", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012

[8] B.Sridhar, K.V.V.S. Reddy, A.M.Prasad," An Unsupervisory Qualitative Image Enhancement using Adaptive Morphological Bilateral Filter for Medical Images", International Journal of Computer Applications, Volume 99 – No.13, August 2014.