Volume: 6 Issue: III Month of publication: March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3367

A Novel Approach for Secret Sharing Using Visual Cryptography

Kajal Samseriya[1], Shraddha Bahadure[2], Sneha Doble[3], Prof. Kunal Purohit [4]
[1, 2, 3, 4] Computer Science & Engineering, Nagpur Institute of Technology, Nagpur, India

Abstract: As compared with the traditional cryptography, visual cryptography decrypts secret images referring to the characteristics of human vision, rather than the cryptography knowledge or complex computations. Furthermore, seeing to the freeness of the secret key, the whole process of encryption as well as decryption for the visual cryptography meets a fast dealing course. As to the security concern, it guarantee that no one can have access to any clues about the content of a secret image from individual cover images. Thus, owing to the studies on this field, the target of light-weighted cryptography is reached. Now the visual cryptography has been developed from the meaningless shadows to the meaningful ones. Seeing to the highly developed technique, some advanced visual cryptography techniques are introduced in this system, respectively.

Keywords: Encryption, Decryption, Security, Image, Pixels Cryptography, AES.

I. INTRODUCTION

The word cryptography is derived from Greek word “Crypto” which means hidden and “Grafo”, which means written. It is the study and implementation of techniques to hide information, to protect a message or text from being read. The information that is protected can be written text, electronic signals, e-mail messages, images or data transmissions. The process of making the information unreadable from the third person is encryption or enciphering and the result of encryption is a cipher text or cryptogram. Reversing this encryption process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so called cipher is used.

Ever since mankind has existed, people have had many secrets, and other people have wanted to know these secrets. The earliest forms of cryptography were performed by paper and pencil, and were available only to those who had access to proper education. Today our lives are completely digitized and cryptography has become an integral part of nearly everyone’s daily life, and it’s used to protect confidential information from hackers. Nearly all our private information is stored in one of the many databases from the government, banks, and health care services, military and so on. Cryptography protects the right to privacy and the right to communicate confidentially. Secure communications can protect one’s intimate private life, business relations, and social or political activities.

The simple architecture in the figure below shows the process of encryption and decryption. Figure [1] is showing the general architecture of the proposed encryption process where an image will select as an input then slicing function will slice image into four equal parts, after that each part will pass from displacement process finally displaced part will be process with proposed encryption algorithm with 128 bits size key value then proposed encryption process will execute number of operation then each encrypted parts of image will be once again combine through combine process and finally a cipher image will produced as an output.

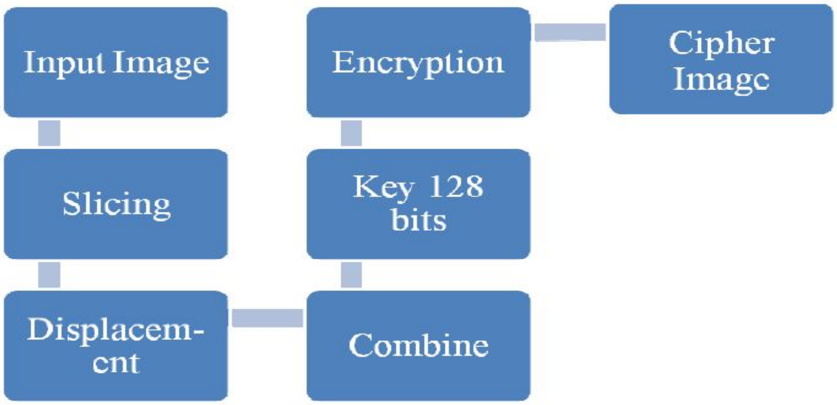


Figure 1: Architecture Diagram for Encryption

Figure 2 is showing the simple architecture of the proposed decryption process where a cipher an image will select as an input then slicing function will slice image into four equal parts then proposed decryption process will execute number of operation with 128 bits size key value. After that each decrypted parts of image will be redisplayed vertically then each parts of image will once again combine and finally an original image will produced as an output.

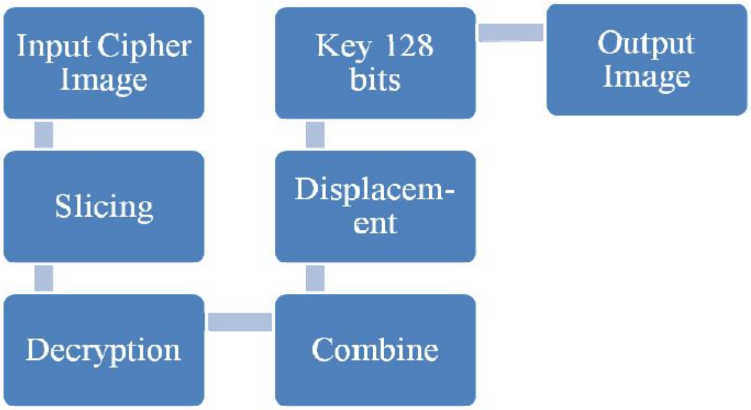


Figure2: Architecture Diagram for Decryption

A. These are five modules in our project they are as follows

1) Convert Text Message Into Image: In first module we convert the text message into images to perform visual cryptography.
2) Slicing of Image: In second module we perform image slicing and shuffle it.
3) Encryption Process: In third module the slicing image will be encrypted and then send it to receiver.
4) Decryption Process: In fourth module the receiver will decrypt the image to see the original image.

II. RELATED WORK

1) Secret sharing in visual cryptography, introduced by Sandeep Katta. In recursive hiding of secrets several messages can be hidden in one of the shares of the original secret image. The images that are to be hidden are taken according to their sizes from smaller to the largest. The first small secret image is divided into five different shares using visual cryptography. Through simulation and analysis, it is demonstrated that recursive hiding and gray scale secret sharing serve as stegnographic channels that can be used to embed invisible watermarks, convey secret keys or encode authentication information.
2) Visual cryptography, introduced by Noar and Shamir is a type of secret sharing techniques for images. The idea of VCS is to split an image into number of shares which separately reveals no information about the original secret image. The image is made up of black and white pixels, and can be recovered by superimposing all the shares without doing any computations. By applying the Noar and Shamir 2-out-of-2 visual cryptography algorithm, two shares are created, which separately produces no information about the original secret image.
3) Dynamic multi-secret sharing scheme, introduced by Han-Yu Lin, and Yi-Shiung based on the one way hash function. If someone wants to share 100 images with others he has to obtain 100 shares, which is difficult to manage. This scheme solves this problem by keeping only one share image and decrypts all other secret images with its share (Universal share).The major characteristics of its design are multi-use of the secret shares and that different group secrets can be reconstructed according to the number of threshold values that provides more flexibility. While applying successive one-way hash functions and the XOR operations, this scheme is secure against serious attacks even though the pseudo secret shares are compromised. Advantage in this scheme is multiple images can be shared easily. In this scheme mathematical calculations are not performed here key safeguarding is missing.
4) Strengthen the Security of Confidential Information using Cryptographic Technique by Prasanna Kumar H.R and Dr. Niranjan N Chiplunkar, are used two methods, in the first method they encrypt the secrete image and then apply the visual cryptography to create the share, in the second method DES is applied and then send to the receiver.
5) Secure visual Cryptography by Shwetha and Paritala Ramanjaneyulu they developed a secret sharing scheme that encodes grey scale images with a limited number of gray levels. The loss in contrast is so large such that the recover image is distorted. In

other methods that construct a visual secret sharing scheme with a general access structure for plural secret images have been proposed.

III.PROBLEM STATEMENT

The common drawbacks of the visual cryptography are we are unable to recover the original input image with good clarity. When no pixels are expanded, a poor quality image is recovered. Sometimes some pixels are lost at the time of decryption. Hence receiver cannot get original data properly. In image encryption process two main problem arises with respect to the time it takes for its computation and its security level. For real time image encryption only for those ciphers are preferable which takes lesser amount of computation time without compromising security an encryption scheme which runs very slowly, even though may have higher degree of security features would be of little practical for real time processes. Hence a trade of has to be made. We are not using lossless compression for encryption or decryption because it also unable to recover the original image with good clarity. There is no algorithm that guarantee the proper recovery of original data.

IV.PROPOSED SYSTEM

In most of the natural images, the values of the neighboring pixels are strongly correlated that is the value of any given pixel can be reasonably predicted from the values of its neighbors. In order to dissipate the high correlation among pixels and increase the entropy value, we propose a newly design image encryption algorithm that divides the image into multiple blocks and then shuffles their positions and then it passes them to the proposed encryption algorithm. By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to using the proposed algorithm alone, and thus improving the security level of the encrypted images. There are two main keys to increase the entropy; the first variable secret key of the displacement process (horizontal and Vertical) and the second variable secret key of the proposed encryption algorithm. The variable secret key of the displacement process determines the constant, which is used to build the secret image with a variable number of blocks. If the key is changed, another constant will be generated, and then a different secret image is obtained. The variable secret key of the proposed encryption algorithm is used to encrypt the displaced image. This encryption process decreases the mutual information among the encrypted image variables and thus increasing the entropy value. In this paper we proposed newly design block-based encryption algorithm where block diagram of proposed system shown in figure [3], in order to increase the security level of the encrypted images.

We propose a newly design image encryption algorithm that divide the image into multiple blocks and then shuffles their positions and then it passes them to the proposed encryption algorithm. The receiver will decrypt the encrypted shuffle image to get the original data.

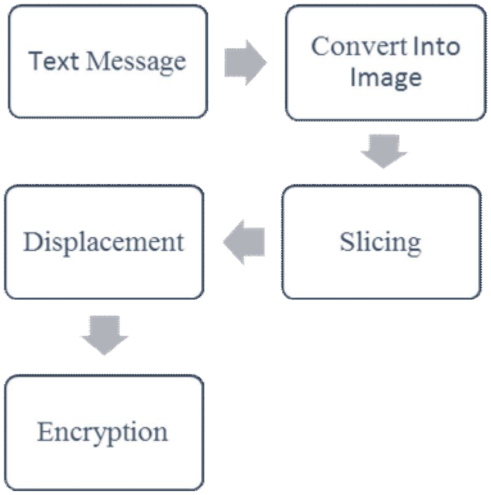


Figure 3: Block Diagram of At Sender Side

Slicing Approach- Here we are performing slicing process as 4 for the purpose of simulation, high performance and easy to understand the concept. Once the slices are update with its new positions. We follow next step. To slicing an image we have used simple concept like select initial X, Y coordinate, maximum X, Y coordinate and intermediate X, Y Coordinate apply mathematic function.

Displacement Approach- After the slicing of image we perform displacement. In the First step original image is sliced and divided into 4 sub slice. This sliced sub image is now used for displacement. Here we are using two displacement approaches (i.e. vertical and horizontal) one by one. This displace of pixel position of sub images reduces the correlation between the adjacent pixels and it may be causes of higher entropy. This approach is being tested by making pixel blocks of different sizes and then their result is being analyzed. For vertical and horizontal displacement of pixel position we have used number of vertical pixel blocks in sub image and accordingly it will explosively displace the pixel blocks in vertical direction in the 1:1 manner; according to this method, block at location 1st will move to 2nd block position, 2nd block will move to 3th block position and 3rd block will to 4th block position. Similarly block at location 4th will move to 3rd block position, 3rd block will to 2nd block position and 2nd block will move to 1st block position. Similarly the above process will apply on horizontal displacement approach. This process will apply on each sub part of image.

V. METHODOLOGY

Proposed Encryption Algorithm: Byte Array containing 16 characters (bytes) long key

Ki denotes ith index in 16 byte long key array

Calculations:

Encryption Side $S1 = (K1\times2) + (K3\times4) + (K5\times6) + (K7\times8) + (K9\times10) + (K11\times12) + (K13\times14) + (K15\times16)$

$S2 = (K0\times1) + (K2\times3) + (K4\times5) + (K6\times7) + (K8\times9) + (K10\times11) + (K12\times13) + (K14\times15)$

Sum = absolute value of (S1+S2)

Compulsory Condition: Value of Sum must always contain exactly three digits e.g. 103,387 etc.

Case-1: if Sum<100 then error message is displayed that the key is too weak.

Case-2: if 100<Sum<999 then it satisfies the condition and therefore further processing takes place as follow:

Step-1: Let Sum = d1d2d3, then RGB values of all the four pixels (P1, P2, P3 and P4) are modified as follow: Perform d1 number of right shifts in R byte of all four pixels Perform d2 number of right shifts in G byte of all four pixels Perform d3 number of right shifts in B byte of all four pixels

Step-2: If d1 is an odd number Reverse the bits in P1 Else Perform EXOR operation between P1 and K1 If d2 is an odd number Reverse the bits in P2 Else Perform EXOR operation between P2 and K2 If d3 is an odd number Reverse the bits in P3 Else Perform EXOR operation between P3 and K3 If d4 is an odd number Reverse the bits in P4 Else Perform EXOR operation between P4 and K4

Case-3: if Sum>999 (i.e. Sum contains more than three digits) then only last three least significant digits are considered and the most significant digit is ignored. It is because most significant (left most) digit has the least possibility of getting changed whereas as we move towards right, digits change rapidly, which is good for encryption process.

Example: Let Sum = d1d2d3d4 Then only d2, d3 and d4 will be considered according to step-2 and d1 will be ignored as the probability of this digit to change is least among d1, d2, d3 and d4.

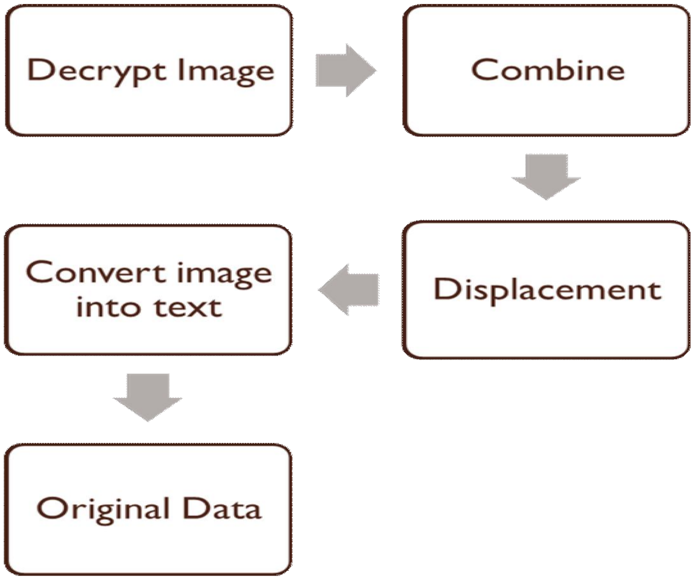


Figure 4: Block Diagram at Receiver Side

Handel Key Exchange Issue: Proposed research is a technique to design and implement of a new Hybrid Image encryption algorithm. Proposed technique is a method of image encryption that combines two or more encryption technique and usually includes a combination of symmetric and asymmetric encryption to take benefit of the strengths of each type of encryption. Symmetric encryption has the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data. However, symmetric encryption has a downside the cryptographic key needs to be known to both the sender and receiver of encrypted data, and it may cause security risk to exchange the key over an insecure channel the. On the other hand, asymmetric or public-key encryption provides better security than symmetric key. In asymmetric key the cryptographic key required for decrypting data does not have to be shared with other parties. This is more secure, but the disadvantage of this encryption is slower computation speed than symmetric key. A solution to this problem is to first encrypt and exchange the symmetric encryption key by means of asymmetric encryption, and then use that symmetric key for encrypting and decrypting the actual data. Although this method provides protection while the encrypted key is transferred between parties, it is not necessarily secure at the moment when the encrypted symmetric key is being decrypted. If an adversary is monitoring the system where this takes place and if the system is not white-box protected, the cryptographic keys can be extracted in plain form. For symmetric key algorithm we will use simple AES algorithm.

VI. IMPLEMENTED WORK

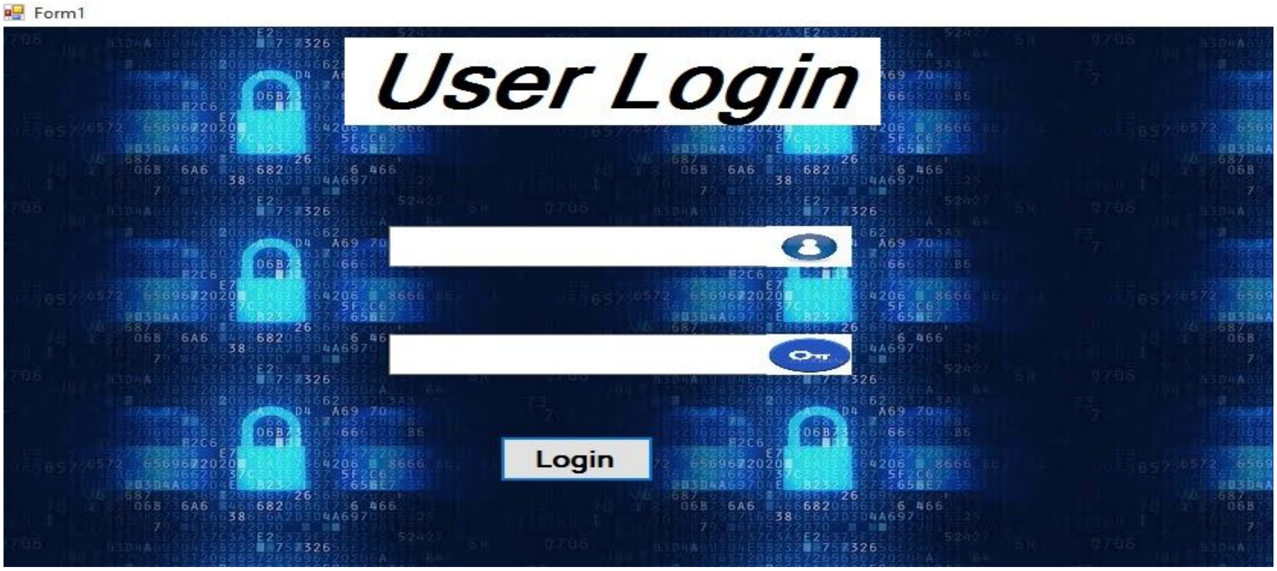
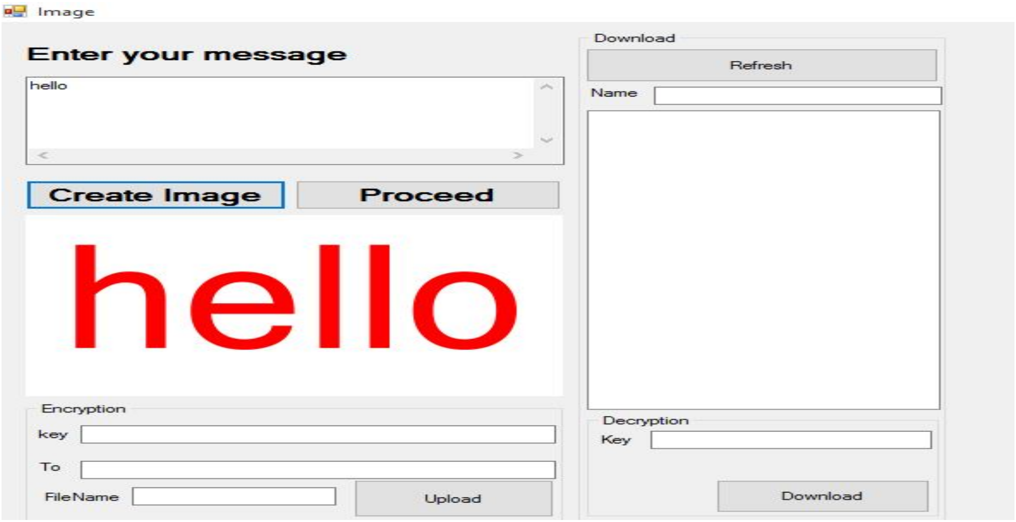
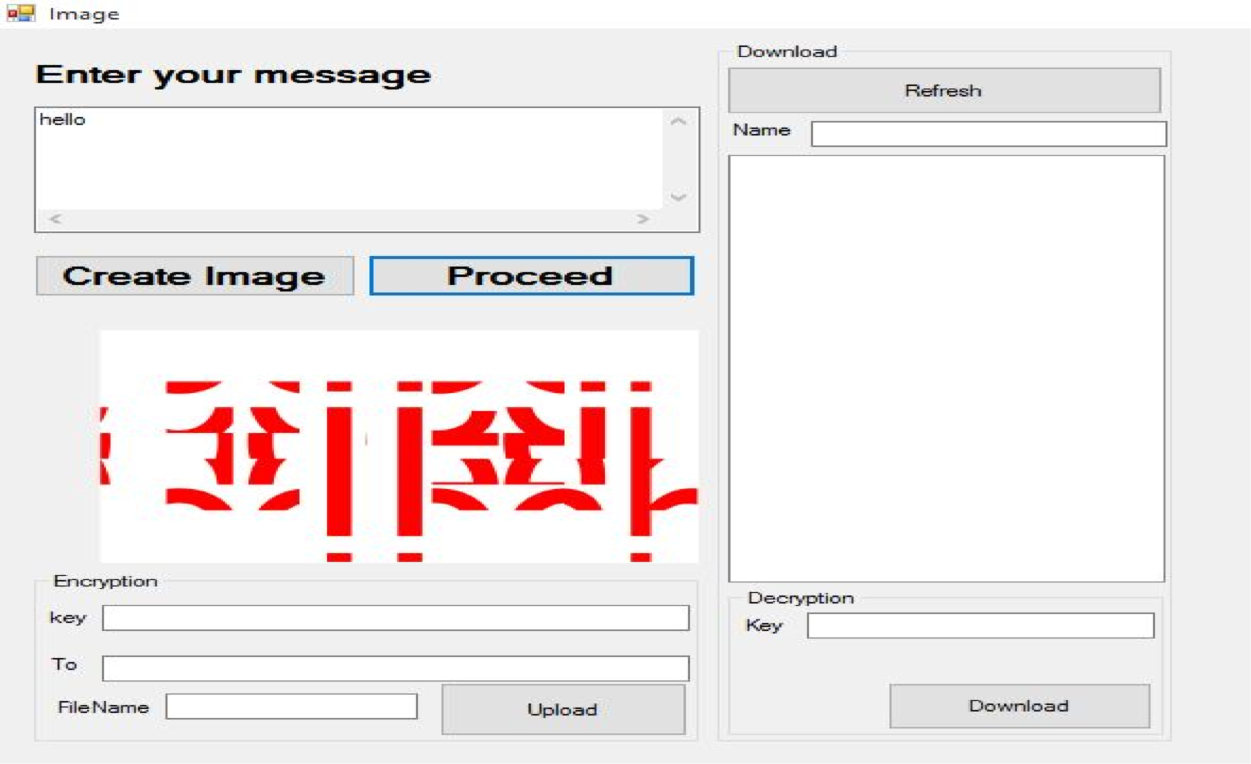


Figure: Login Form



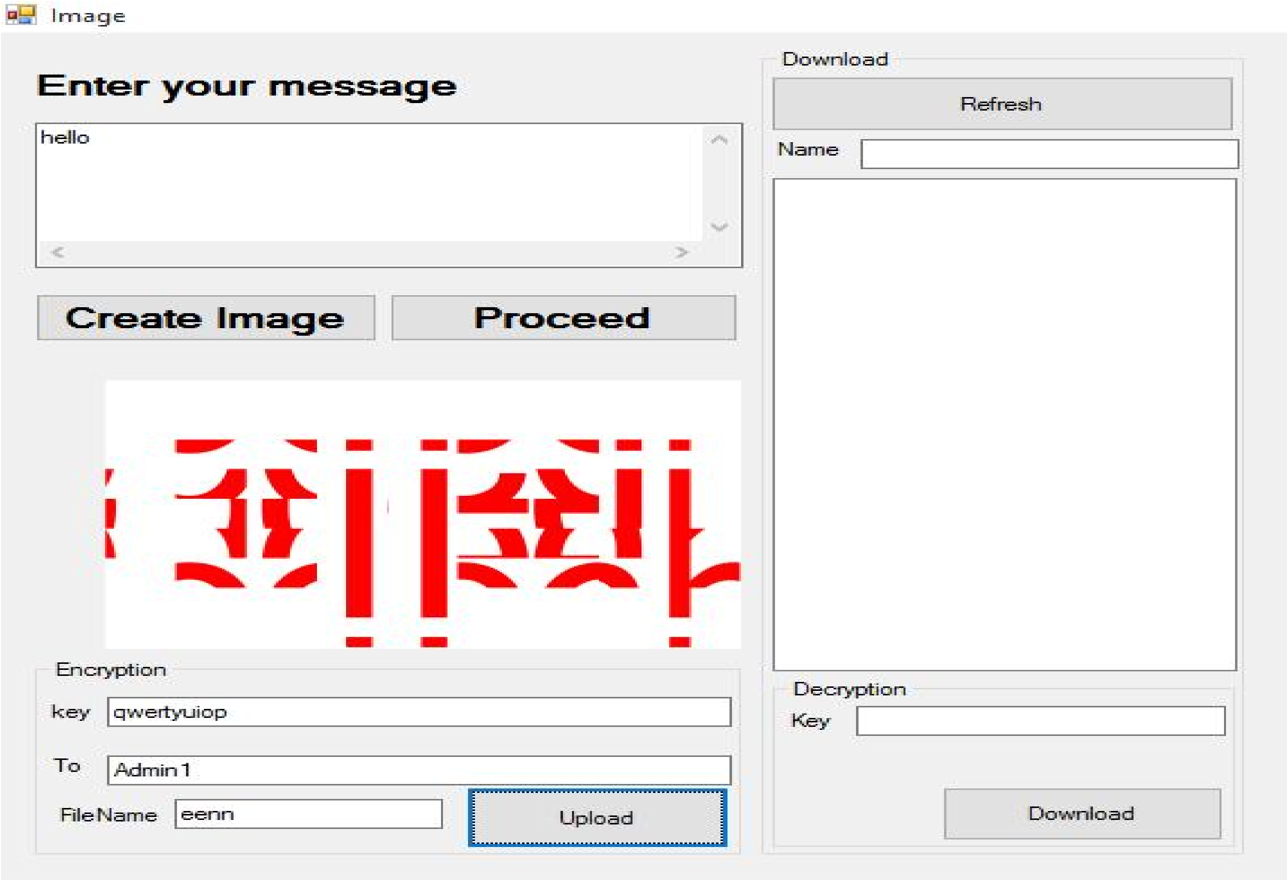
Enter your message
hello

Figure: Convert Text Message Into Image



hello

Figure: Slicing Of Image And Shuffle Their Position



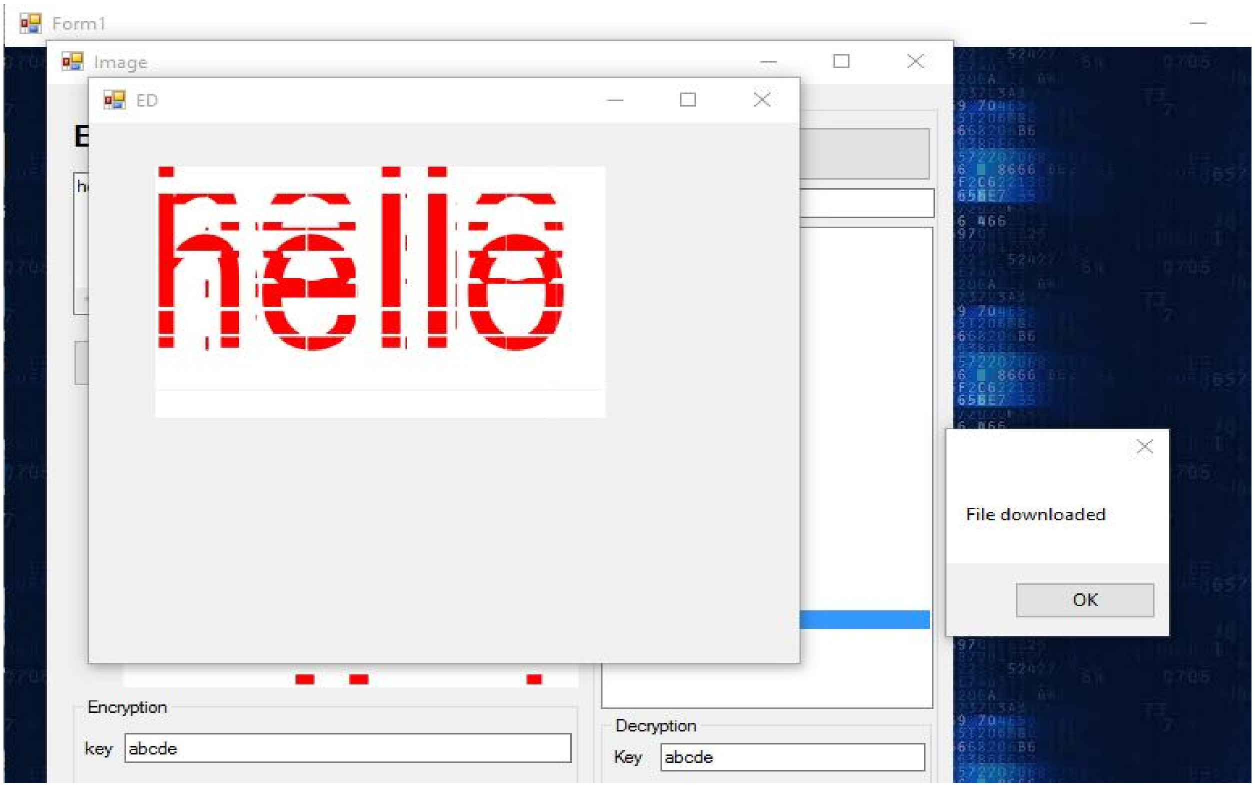
hello

key qwertyuiop

To Admin1

FileName eenn

Figure: Encryption Of Image



File downloaded

key abcde

Key abcde

FIGURE: DECRYPTION OF IMAGE

VII. CONCLUSIONS AND FUTURE SCOPE

Visual cryptography is a technique to provide a secure way to transfer images. The main advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation require. Visual Cryptography allows easy decoding of the secret image by a simple stacking of the printed share transparencies. However, there are some practical issues that need careful consideration. The transparencies should be precisely aligned in order to obtain a clear reconstruction of the secret image. There is also some unavoidable noise introduced during the printing process. Furthermore, the stacking method can only simulate the OR operation which always leads to a loss in contrast. The loss of contrast can be rectified by further processing.

As visual cryptography schemes operate at the pixel levels, each pixel on one share must be matched correctly with the corresponding pixel on the other share. Superimposing the shares with even a slight change in the alignment results in a drastic degradation in the quality of the reconstructed image.

REFERENCES

[1] Secret sharing using visual cryptography by Renu Poriye and Dr. S. S Tyagi, Manav Rachna International University, 2014.

[2] New visual secret sharing schemes using probabilistic method by Ching-Nung Yang, National Dong Hwa University, 2004.

[3] Secure visual cryptography by R. Yadagiri Rao, RVR Institute of Engineering and Technology, Ibrahimpatnam, 2013.

[4] Strengthen the Security of Confidential Information using Cryptographic Technique by Prasanna Kumar H.R and Dr. Niranjan N Chipkunkar.

[5] A new Image Encryption Algorithm Based Slicing and Displacement Followed By Symmetric and Asymmetric Cyptography Technique by Anita Maheshwari, M.E Scholar JIT Khargon, 2015.

[6] Pooja, Dr. Lalitha Y. S,"Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication",International Journal of Engineering Research and Development, Volume 10, Issue 6, June 2014.

[7] Gayathri.D, Dr.T.Gunasekran, "Design of XOR based visual cryptography scheme", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Volume 4, Issue 2, February 2015.

[8] Isha Padiya, Vinod Manure, Ashok Vidhate , "Visual Secret Sharing Scheme Using Encrypting Multiple Images", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 1, January 2015.

[9] Mary Shanthi Rani, Germine Mary, "MSKS for Data Hiding and Retrieval using Visual Cryptography Images", International Journal of Computer Applications, Volume 108 – No. 4, December 2014.

[10] Mr. Praveen Chouksey, Mr.Reetesh.Rai, "Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space", IRACST - International Journal of Computer Science and Information Technology & Security(IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015.