IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 2, Ver. II (Mar-Apr. 2014), PP 38-45
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Novel Spatial and Transform Domain Image Encryption Algorithms

T. Sudha[1], B. Gopi[2]
[1]*Professor & HOD, Dept. of CSE & IT, Sri Padmavati Mahila Viswa Vidhyalayam, Tirupati*
[2]*Research Scholar, Dept. of CSE, Vikrama Simhapuri University, Nellore*

Abstract: *Image encryption has been crucial for many applications where the secret image consisting of secrete information regarding an application will be embedded in another data preferably image. New technology and new applications bring threat to the information. To provide security to the information with respect to new threats, new algorithms need to be devised. In this paper three techniques for image encryption are proposed. In the first, the secret image will be embedded into least significant bit position of another image called carrier or source image. But the order with which the insertion takes place will be decided by a polynomial, somehow similar to the hash table insertion. In the second, the secret image is hidden in the decomposed data of multimedia data. The first technique is a spatial domain technique, whereas the second is a transform domain technique. In the third, the secret image will be split into share images. The share images will be hidden in another image. By using the above techniques different levels of security is provided to the information.*

Keywords: *Image encryption, LSB, Multistage encryption, Wavelet domain*

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed. A secure computing environment would not be complete without consideration of encryption technology. The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it.

The use of simple codes to protect information can be traced back to the fifth century BC. As time has progressed, the methods by which information is protected have become more complex and more secure. Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection. Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data. To help understand between the two forms of data, the data before encryption is called the plaintext and the encrypted data as ciphertext. The security of encryption lies in the ability of an algorithm to generate ciphertext from which the original plaintext can’t be separated easily.

In a very simple example, encryption of the word "secret" could result in "terces." Reversing the order of the letters in the plaintext generates the ciphertext. This is a very simple encryption - it is quite easy for an attacker to retrieve the original data. A better method of encrypting this message might be to create an alternate alphabet by shifting each letter by some arbitrary number. This is known as a substitution cipher, a form of encryption that is still used in puzzle books today. For example, encrypting the word "secret" with an alphabet shifted by 3 letters to the right produces "vhfuhw”. A substitution cipher simply exchanges one letter or word with another. This particular algorithm is called the "Caesar Cipher". In the quest for a more secure method of protecting information, the introduction of a key adds another level of security. A key is a piece of information that allows only those that hold it to encode and decode a message.

Keys come in many different forms such as passwords, numbers generated by an algorithm, digital fingerprints and even electronic devices that work like door keys. It is a series of numbers or symbols that are used to encode a message so that it can only be read by someone in possession of that key or a related key. A key allows both the sender and the recipient of the message to understand how the message has been encrypted and assures them that nobody else knows how it has been encrypted. It is the key that enables the recipient to properly decode the message. Using the previous example of a substitution cipher, anyone who knows the Caesar Cipher can decrypt all messages encrypted with it, regardless of who actually encrypted the message. One could strengthen the substitution cipher with a key, by choosing an arbitrary number and using that as the number of letters by which to shift when creating their alternate alphabet. That number therefore becomes the key by which the message is unlocked. The individual who is sending the message communicates the key to the recipient of the message, allowing them to unlock it. One disadvantage of this system is that an attacker can decrypt the message if the key is intercepted. To protect the key, encryption can be used during communication or the key can be sent in a separate communication.

The rest of the paper is organized as follows. The next section reviews different encryption techniques in literature. The section III presents an LSB based spatial domain technique. In the section IV a discussion of wavelet based transform domain encryption technique is presented. Section V discusses a two stage encryption algorithm based on shares and LSB replacement. Section VI concludes this paper.

II. RELATED WORK

In the literature a number of works are published on image encryption. In this section, some of works are mentioned. Haojiang Gao et. al, in [1] presented a new chaotic algorithm (NCA) for image encryption which uses power function and tangent function instead of linear function. Its structural parameters are obtained by experimental analysis. And an image encryption algorithm in a one-time-one password system is designed. The experimental results demonstrate that the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. Komal D Patel et. al, in [2] presented a survey of different encryption techniques.

In [3] A. Mitra et. al proposes a new approach for image encryption using a combination of different permutation techniques. The main idea behind this work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. An approach for a random combination of the aforementioned permutations for image encryption is presented. From the results, it is observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. A random combination method employing all the three techniques thus is observed to be useful for tactical security applications, where protection is needed only against a casual observer.

In [4], Mohammad. A. B. Younes et. al introduced a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

In [5], Anil Kumar Yadav et. al, presented complexity analysis of image encryption/decryption scheme. The proposed scheme is especially useful for encryption of large amounts of data, such as digital images. First, a pair of keys is given by using matrix transformation. Second, the image is encrypted using private key in its transformation domain. Finally the receiver uses the public key to decrypt the encrypted messages. This scheme satisfies the characters of convenient realization, less computation complexity and good security.

The salient features of the proposed image encryption method are loss-less, symmetric private key encryption, a very large number of secret keys, and key-dependent pixel value replacement. Ismail Amr Ismail et. al, in [6] introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. The external secret key is used to derive the initial conditions for the chaotic maps, and is employed with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the pixels are encrypted using an iterative cipher module based feedback and data-dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information. To make the cipher more robust against any attack, the secret key is modified after encryption of each pixel of the plain image. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

Manjunath Prasad et. al, in [7] presented a chaos based encryption algorithm for images. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algorithm is tested with two different maps and performance analysis is done to select best suited map for encryption. Reza Moradi Rad et. al, in [8] proposes a new framework for image encryption, a layer based method combining some most efficient image encryption algorithms. It is tried to take all encryption concerns into consider, achieve highest possible level of security while cost is already acceptable. The proposed method provides different security level to blocks of varied significance in image to consume less computational resources. Various analysis and experiments such as histogram, correlation coefficient, entropy, and computational time revealed that significant promotion in security has been achieved without compromising on the computational time.

Pooja Mishra et. al in [9] presents survey on methods for protecting the distribution of digital images in an efficient and secure way. The main focus is survey of various encryption methods in which image is divided into small parts for encryption to increase security level of encryption techniques. Sonam Pathak et. al, in [10] survey several image encryption techniques with their flaws and advantages; based on survey some future suggestions of image encryption made, which may provide better security enhancement in the case of various types of images. The chaos based crypto system for better analysis with data encryption standard (DES) encryption was also discussed. In this paper three image encryption algorithms are proposed. These are LSB based technique, Transform domain technique and share based two stage encryption algorithms.

III. LSB REPLACEMENT TECHNIQUE

Redundancy is one of the major aspects of creation. A close inspection reveals that redundancy does exist, and exists in abundance. Computer files are not an exception to this fact. For instance an image on a computer is represented by large number of pixels, which in turn have much redundant information. The simplest technique is to use the redundant bits so as to do the covert communication. For e.g. each pixel of an image consists of a variation of all three primary colors red, green and blue, in a standard 24-bit bitmap, requiring 8 bits each for these three colors, i.e. there are 256different variations, ranging from 00000000 to 11111111, for each color in a pixel. So, to represent the color white, the code would look like 11111111 1111111111111111. But, the human eye cannot distinguish the difference between too many colors, the colour11111110 11111110 11111110 would look exactly the same as white, which means that the last digit in every bit in every pixel could be changed without much visual degradation of quality.

This is the basis of the Least Significant Bit Insertion technique. We require 8 bits to represent one pixel in a gray scale image and there are three potential slots extra in every pixel of a picture. Therefore, in a conductive environment, with every three pixels, one pixel of a gray scale image could be concealed. The current study took windows bit map image file format with loss less compression in to consideration. The proposed algorithm would require a secrete message in the form of an image (M), a cover image (C) and a pseudorandom seed Generated by polynomial (S) as input.

In Windows bit map format, every image will have three separate color channels; a channel dedicated for the red component (rCom), another one for the green component (gCom), and a third one for the blue component (bCom). But one question arises here that in what order the pixels from secrete image should be placed in cover image? A polynomial is going to be used, from which the location or the cover image pixel identification will be provided to the encoder, so that the encoder embeds the secrete image data into suitable and noted locations of the cover image. The same polynomial will be used at the decoding side to find the locations where the secrete image data is embedded. Consequently, the decoder will decode the secrete image data from the information provided by the polynomial. The encoding and decoding processes are depicted in figures 1 and 2.

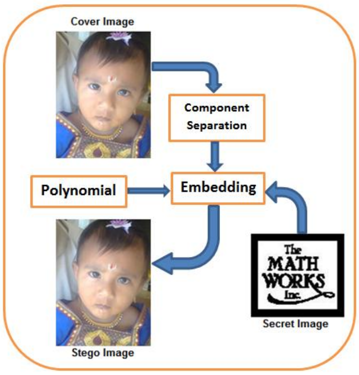


Fig. 1 Encoding process of LSB based technique

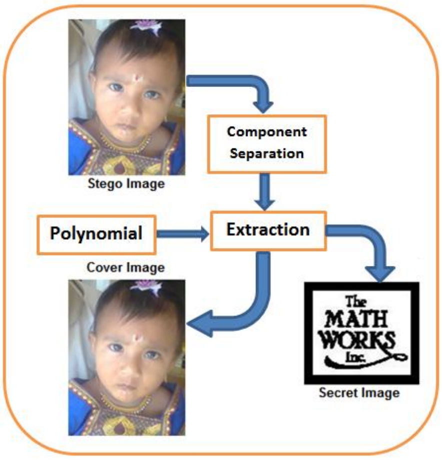


Fig. 2 Decoding process of LSB based technique

IV. TRANSFORM DOMAIN TECHNIQUES

In the previous section LSB based technique is presented. To store one pixel's information of secret image, eight pixels of cover image are required. Hence to hide an image of dimension say 256X256 (total number of pixels is 65536), a cover image with 524288 pixels is required. It means that the cover image dimension should be 1024X512 or 600X900. This image need to be transmitted to the decoding end to extract the secrete data. This is the limitation of the LSB based techniques. The input or cover image should be so large so that by using only one of eighth of its memory it has to store the secret image. In the transform domain technique the transformed representation of some multimedia can be utilized to hold the secret image information. The transformation considered in this work is wavelet transform with db4. The transformed information is again stored as numbers only. Hence in these numbers the LSB as well as some of data will not be useful because of redundancy as well as duplicate data. The discrete wavelet transform of an audio signal is calculated. The secrete image is embedded in the wavelet domain of the audio signal. The sequence of steps followed to encrypt the secret image in the wavelet representation of the audio signal is given below.

Step 1. Consider the audio signal sampled with the sampling rate of 11025 Hz.

Step 2. The audio signal is divided into frames with 1024 samples. Decompose every frame of the speech signal using 'db4' wavelet transformation. Hide the first bit of the binary data collected from the binary image into the third level detail coefficients obtained using wavelet decomposition of the first audio frame. This is done by changing the values of the third level detail coefficients such that mean of the third level detail coefficients is modified to 'm+k' if the binary value is '1' or to 'm-k' if the binary value is '0'.Note that variance remains same. The variable 'm' is the mean of the fifth level detail coefficients. The value for the constant 'k' is chosen as 1/5th of the energy of the third level detail coefficients.

Step 3. This is repeated for the other frames of the speech signal for hiding the entire bits obtained from the binary image.

Step 4. Thus Binary image is hidden in the wavelet domain of the audio signal.

Step 5. The hidden binary data is retrieved by comparing the mean of the corresponding detail coefficients computed before and after hiding. If the mean of the third level detail co-efficient of the particular frame corresponding to the original signal is greater than the mean of the third level detail coefficients of the respective frame corresponding to the watermarked signal, the bit stored is considered as '1', otherwise '0'.

Step 6. Note that the duration of the audio signal is chosen such that all the binary data collected from the binary image are hidden in the audio signal.

In this work length of the audio signal used for hiding binary image data is 11488 samples. It is repeated 100 times so that the length of the audio signal becomes 1148800 samples. The size of the Binary image used is 45X45.Binary image is stored at the rate of 1 bit in 256 samples of the audio signal.

V. SHARE BASED TECHNIQUES

Noar and Shamir proposed the first visual secret sharing scheme of them all in 1994. Instead of the traditional cryptographic methods that require complex computation, Noar and Shamir's scheme uses human visual system to decrypt the secret image. Furthermore, the scheme they proposed is a (k, n)-threshold visual secret sharing scheme. In other words, this method generates as many as n meaningless images called shares out of the secret image, and to decode the secret image requires as many as k, where k ≤ n, or more shares printed out on transparencies and stacked together.

Otherwise, there is no way the secret image can be revealed out of the shares. In a (2, 2)-threshold visual secret sharing scheme, let the secret image be a binary image with size N×N. To begin with, every pixel is extended into a 2×2 block, and each block is composed of two black pixels and two white pixels as Fig. 3 shows. By referring to a predefined coding table, a block can be produced by corresponding to a related pixel of the secret image. When all the secret pixels are done processed, that is the moment the two shares are generated. Stacking the two shares together, we can reveal the secret image. After the encoding process, the size of the shares becomes 2N×2N. The following are the secret image pixel coding rules.

First, the system randomly picks one block from the six shown in Fig. 3 to represent Share 1 block. Second, a pixel is found that conforms to the secret image, and then the coding rules in Table 1 will be compared so that a matching block of Share 2 can be generated. When all the pixels are done processed, there will be two 2N×2N shares. Finally, stacking the two shares together, we can reveal the secret image. As effective and ingenious as this scheme may be, however, it can only process one secret image at a time, and the secret image can only be either text or a simple black-and-white design.

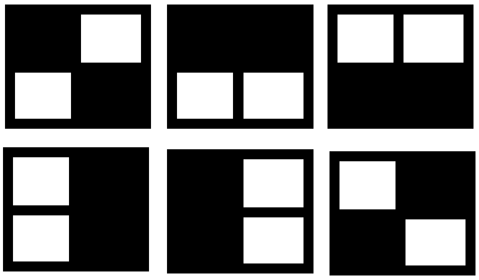
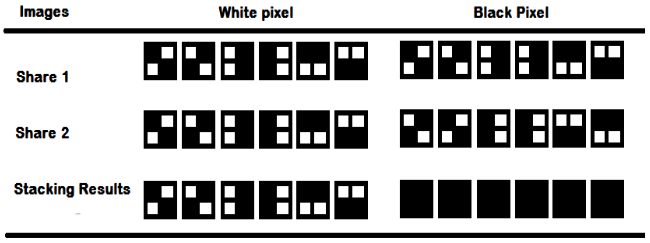


Fig. 3 Block group

TABLE I: Coding Table of Share Blocks


Images
White pixel
Black Pixel
Share 1
Share 2
Stacking Results

In this paper a new scheme for visual cryptography is proposed which will use watermarking technique to embed the generated shares into any cover image. Proposed scheme includes three phases described in this section. Phase I - Visual Cryptographic Encryption: In the first phase we will do visual cryptography encryption. It consists of generation of shares using any of the basic visual cryptography models. In our proposed scheme, a (2, 2) Visual cryptography share creation is performed. Each pixel in the secret image is divided into four sub pixels. A complete white pixel is shared into two identical blocks of four sub pixels. A complete black pixel is shared into two complementary blocks of four sub pixels. All the pixels in the secret image are encrypted similarly using this scheme. The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey.

When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black). The visual secret sharing scheme assumes that the message consists of a collection of black and white pixels and each pixel is handled separately. 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 by an n × m Boolean matrix S = $[s_{ij}]$ where $s_{ij} = 1$ if the j^{th} sub pixel in the i^{th} transparency is black. When transparencies in S. The grey level of this 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 users as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$.

Phase II - Hiding the Shares using Digital watermarking: This phase embeds image shares into some cover images using digital watermarking. This phase results different meaningful shares consist some cover image. Discrete cosine transformation (DCT) is used for convert the image into frequency domain. DCT can be interpreted as decomposition into a set of frequency coefficients having the same bandwidth on a logarithmic scale. The obtained coefficients are real number values. The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. The algorithm for embedding the watermark is following.

```
Step 1: Set minimum coefficient difference.
Step 2: Set the size of the block in cover image to be used for each bit in watermark.
Step 3: Read in cover object.
Step 4: Determine size of cover image.
Step 5: Determine maximum message size based on cover object and block size.
Step 6: Read in the message image.
Step 7: Reshape the message to a vector.
Step 8: Check that the message is not too large for cover.
Step 9: Pad the message out to the maximum message size with ones.
Step 10: Process the image in blocks.
Step 11: Transform block using DCT.
Step 12: If message bit is black then value of frequency coefficient (5, 2) > (4, 3).
Step 13: End if
Step 14: If message bit is white then value of frequency coefficient (5, 2) < (4, 3).
Step 15: End if
Step 16: Adjust the two values such that their difference >=k.
Step 17: Transform block back into spatial domain.
Step 18: Move on to next block, at the end of row move to next row.
Step 19: Exit
```

Phase III - Visual Cryptographic Decryption: In this phase the binary watermarked shares extracted from the host images. The proposed watermarking scheme does not require original image or any of its features for the extraction of watermark, and hence this scheme is blind. Then we apply the visual cryptographic decryption. As we know that visual Cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. Now we can decrypt the original secret image by overlapping or stacking the shares. The algorithm for watermark extraction is following.

```
Step 1: Set the size of the block in cover to be used for each bit in watermark.
Step 2: Read in the watermarked object.
Step 3: Determine size of watermarked image.
Step 4: Determine max message size based on cover object and block size.
Step 5: Process the image in blocks.
Step 6: Transform block using DCT.
Step 7: If dct_block (5, 2) > dct_block (4, 3) then message bit is 0, otherwise message bit is 1.
Step 8: End if
Step 9: Move on to next block, at the end of row move to next row.
Step 10: Reshape the embedded message.
Step 11: Exit
```

The Fig. 4 shows the input image. The share-1 and share-2 mentioned in the above section for the mentioned input image is calculated to be as shown in the figure 5. The shares are embedded to provide second stage security. The share images are gray scale images. Hence these images can be easily hidden by a big color image. The process is depicted in the figure 6.

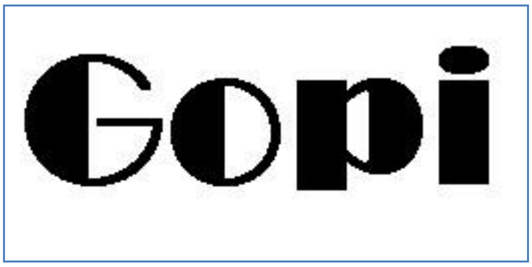


Fig. 4 Input Image

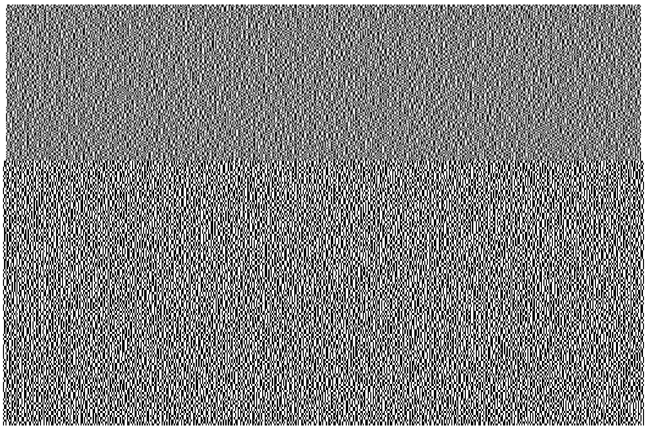
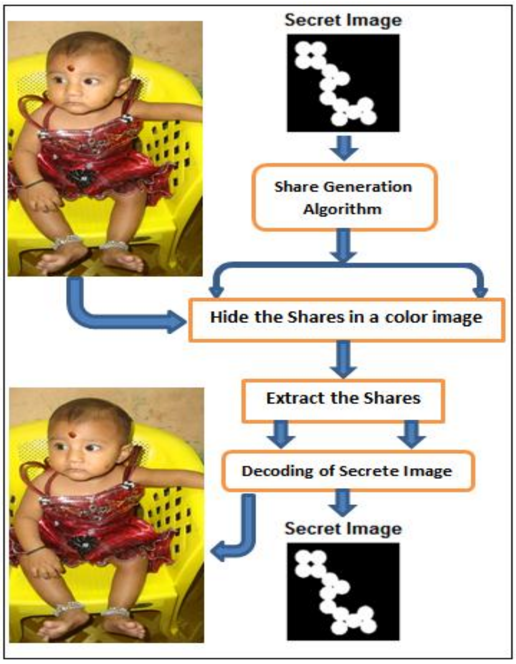


Fig. 5 Share Images After Embedding the Share of Secret Image



Secret Image
Share Generation Algorithm
Hide the Shares in a color image
Extract the Shares
Decoding of Secrete Image
Secret Image

Fig. 6 Two stage image encryption scheme

The share images are extracted from the cover image. The overlapping of these share images retrieves the original input image which is shown in Fig 7.

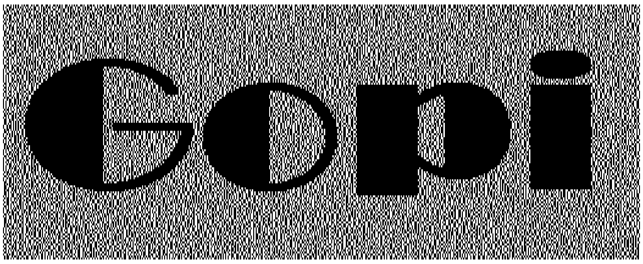


Fig. 7 Reconstructed image by overlapping the Share Images

VI. CONCLUSIONS

Image encryption has been a crucial task in the modern era. The reason behind is efficient intruder and unlock algorithms developed by the spurious users of the computer technology. In the literature many algorithms for image encryption are proposed. In this paper three image encryption algorithms are proposed. The first, spatial domain technique performs spatial domain operations on image to hide the secret image in cover image. To incorporate more robustness, the transform domain techniques are proposed. The wavelet domain technique hides the secret image in the decomposed data of cover image. The bits of decomposed data which can be retrieved by using other bits are used to hide the secret image. The third method is a two stage encryption algorithm. In the first stage the secret image should be decomposed into two share images. In the second stage of the share images will be embedded in a cover image. The inverse operations will be performed to extract the secret image from the cover image. It is observed that the proposed techniques improve the security of secret image.

REFERENCES

[1] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, “A new chaotic algorithm for image encryption”, Chaos, Solitons and Fractals, Elsevier 29 (2006) 393–399

[2] Komal D Patel, Sonal Belani, “ Image Encryption Using Different Techniques: A Review”, International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 1, November 2011.

[3] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, “A New Image Encryption Approach using Combinational Permutation Techniques”, International Journal of Electrical and Computer Engineering 1:2 2006.

[4] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 2008.

[5] Anil Kumar Yadav and Ravinder Kumar Purwar, “Complexity Analysis of Image Encryption Technique”. UFL & JIITU, IC3–2008.

[6] Ismail Amr Ismail, Mohammed Amin, and Hossam Diab, “A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps”, International Journal of Network Security, Vol.11, No.1, PP.1-10, July 2010.

[7] Manjunath Prasad and K.L.Sudha, “Chaos Image Encryption using Pixel shuffling”, D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011.

[8] Reza Moradi Rad, Abdolrahman Attar and Reza Ebrahimi Atani, “A Comprehensive Layer Based Encryption Method for Visual Data”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 6, No. 1, February, 2013.

[9] Pooja Mishra, Biju Thankachan, “A Survey on Various Encryption and Key Selection Techniques”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 7, January 2013.

[10] Sonam Pathak, Rachana kamble, “A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique”, International Journal of Advanced Research in Computer and Communication Engineering Volume 2, Issue 7, July 2013.

Prof. T Sudha is currently working as Professor and Head of the Department, Dept. of CSE & IT in Sri Padmavathi Mahila Viswa Vidhyalayam, Tirupati. She has held many positions in Sri Padmavathi Mahila Viswa Vidhyalayam as well as other institutes like Vikrama Simhapuri University, Nellore. She did M.Sc., M.Phil., Ph.D and MS all on Computer Science field. She has published a number of research papers in national and international journals.

B. Gopi received Masters in Computer Science and Applications and Masters in Technology from SV University, Tirupati and Acharya Nagarjuna University, Guntur respectively. He worked as Senior Lecturer in the Department of Computer Science and Applications in Sri Karunamayi Institute of Higher Learning, Gudur from 2007 to 2010. Currently he is a full time research scholar at the Department of Computer Science in Vikrama Simhapuri University, Nellore. His research interests include Fractal theory, Image Encryption.