ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

A Visual Secret Sharing Technique for Secure and Fast Transmission of Image

Shruthi H R[1], Ranjan Kumar H S[2], Prasanna Kumar H R[3]

[1]II[nd]year M.Tech, Dept. of C.S., NMAMIT, Nitte, Karnataka, India

[2]Assistant Professor, Dept. of C.S., NMAMIT, Nitte, Karnataka, India

[3]Assistant Professor, Dept of C.S., PESITM, Shimoga, Karnataka, India

ABSTRACT: In the advent of booming communication technology, the needs for information sharing and transfer have increased exponentially which requires more and more new techniques to meet the increasing needs of a modern society. Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Random grid based technique is a non expanded visual cryptographic technique for generating both meaningless and noise like shares. In this paper the idea is to increase the levels of security and to enhance the transmission speed of secret information over the network, as the basic model of Visual Cryptography is not an efficient tool to hide the information. In the proposed scheme initially the image is encrypted by Visual Cryptography using Random Grids and we propose a technique using combined DCT based Compression with Steganography for the speed transmission and additional security of encrypted random image shares over the transmitting media. The experimental results demonstrate the feasibility of the proposed scheme.

KEYWORDS: Visual cryptography; Compression; DCT; Random grid; Shares; Steganography

I. INTRODUCTION

In the recent communication technology, the needs for information exchange and transfer have increased exponentially. In the public domain the threat of an intruder accessing secret information has been an ever existing concern for the data communication. Steganography, Cryptography, and Visual cryptography are the most widely used techniques to overcome these threats.

In Cryptography the plaintext is transformed (*encrypting* it) into an unreadable format, which is called as called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. In steganography a message, image, or file is embedded within another message, image, or file. Both these techniques provide some level of security of data. In VC the image is encrypted by creating random shares and decryption is done by human eyes. However, neither of them alone is secure enough over an unsecure communication channel for sharing information and is vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security, in order to minimize the threat of intrusion we still need a highly secured system to transfer information over any communication media.

For any communication system, a secure transmission of information can be achieved using a powerful encoding algorithm and a fast transmission to send the information from a transmitter to a receiver (that can be done using an efficient compression technique) is two important requirements. To satisfy these constraints, we propose a new method of compression and encryption at same time.

The image is initially encrypted by visual cryptography using random grid scheme by generating random shares. Then we cover the random share with a cover image. Our proposed method is based on the hiding of information (Embedding) in the transmitter side and taking out (Extracting) algorithm in receiver side the decoding phase. In addition we would like to compress the transmitting data, to achieve a high speed communication.

For this purpose Discrete Cosine Transform (DCT) is utilized because most of the power is concentrated in the lower frequency bands by DCT, it is used to cut out the higher frequency components. Then the compressed DCT elements are rotated, the rotations have another aspect. The directions and degrees of the rotations are saved as “key” to restore the original images. If the receiver does not know “key,” it is hard to recover the original images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

The digital embedding method proposed for hiding an image into another image helps to maintain the quality of the reconstructed image. The image file, which is to be hidden, is termed as Target Image (share image) and the image behind which it is to be hidden is termed as Cover Image. In this paper the whole process is divided into transmitter side process and receiver side process.

II. RELATED WORK

Visual cryptography (VC) is a novel concept first introduced by Naor and Shamir [1] in 1994. VC allows one or more images to be encrypted and subsequently decrypted. In VC decryption of an image encrypted by a visual cryptography scheme requires no mathematical computations or knowledge of cryptography. Instead, the original image becomes visible to the naked eye simply by overlaying cipher transparencies known as shares created during the encryption process. In the (k, n) VC scheme ($2 \leq k \leq n$), the secret image is encoded into n transparencies, called shares, only if at least k shares are superimposed together can reveal the secret image, but no information can be obtained by any less than k shares. Ateniese et al. proposed the Extended Scheme for Visual Cryptography (EVCS) which allowed for meaningful content in the cover-image to appear on the share-image [2]. However VC uses pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are image distortion, wastage of storage space, and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several researches making efforts to deal with the pixel expansion problem. Most of these have fallen into the category of probability visual cryptography schemes. Random Grid Encryption Algorithms for Binary Images Was proposed by Kafri and Keren [3] aiming at the minimization of the pixel expansion. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. In 2007 Shyu [4] extended Kafri and Keren's RGVSS model, he proposed three different models utilizing a (2, 2)-threshold scheme. Shyu [5] and Chen and Tsao [6] also discussed about (2, *n*) - and (*n*, *n*)-threshold RGVSS schemes, so this method is no longer limited to the (2, 2)-threshold scheme. Transmission of a meaningless image can arouse the suspicion of an intruder, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus decreasing the security of the share-image. Ateniese et al. [7] first applied the strategy of steganography to generate meaningful share-images in VC. Following Ateniese, Chang et al. [8] found a way to hide a color secret image in two color cover images. Thien and Lin [9] introduced a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of visual cryptography which is decryption directly by the human eye.

Many researches were carried out to combine the encryption and compression technique, to reduce the amount of space required to store the secret data, for faster communication and better security of secret data. Andrew B. Watson introduced Image Compression Using the Discrete Cosine Transform in 1994[10]. A. Alfalou C. Brosseau et al. [11] performed compression based on the discrete cosine transform (DCT). Two levels of encryption are used. The first one is due to the grouping of the DCTs in the spectral domain and after a second transformation, i.e. to hide the target images; one of the input images is used as encryption key. The compression is better than JPEG in terms of PSNR. Maher Jridi, Ayman Alfalou [12] presented a method that utilizes the DCT properties to achieve the compression and the encryption simultaneously. First for compression, 8-point DCT applied to several images. Second, only some special points of DCT outputs are multiplexed. For the encryption process, a random number is generated and added to some specific DCT coefficients. Image Encryption Using DCT and Stream Cipher were proposed in 2009[13]. The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients correlated to the higher frequencies of the image block are encrypted using Non-Linear Shift Back. New Image Encryption and Compression Method Based on Independent Component Analysis were proposed in 2007[14]. In this new method is proposed combining encryption and compression based on ICA and Discrete Cosine Transform (DCT). In this paper a combination of steganography, random grid visual cryptography and DCT based compression technique is applied in order to achieve the higher security levels and for faster transmission of information.

III. APPROACH

Flow of our approach to transmit encrypted and compressed images to approved folks is illustrated. In the encryption stage the image is encoded into two shares by applying random grid visual cryptographic scheme (RGVCS).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

The shares have same size as that of original image. Then, we are dividing the share images into tiny blocks and apply two-dimensional Discrete Cosine Transform (DCT) separately of every block.

With the property of the DCT transform that regroup the vital data within the upper-left corner; we are able to simply choose this desired data by applying an easy low pass filter to compress them. Thus we can cut back the size of data to be transmitted. After the choice of desired info, we'll encode them by grouping along (merging) the information coming back from many DCT parts of the images within the spectral plane. As a result of the DCT components of natural images have high energy in lower frequency bands; DCT parts of various sources might not be independent. To resolve this downside and acquire associate freelance version of those DCT parts, we have a tendency to rotate every DCT block at random. Moreover, the rotation operation is going to be used as associate adding secret writing key. This latent key should be sent to the receiver so as to build the decrypted images. Then the compressed image is embedded in random cover image using LSB technique. In LSB based Steganography the secret data is embedded in to the least significant bits of the pixel values in a cover image.

In the decryption stage we extract the original image from the cover image this process is termed as extraction. Then the DCT components are rotated and decompressed based on the information of the encryption keys. In the next step we apply Inverse Discrete Cosine Transform (IDCT) to the reconstructed DCT components to obtain the original share images. Finally the share images are overlapped to obtain the original image.

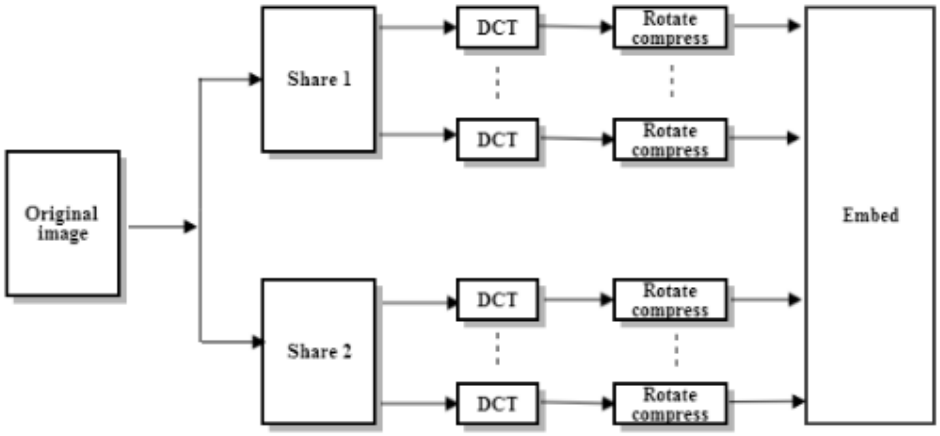


Fig.1. Transmission side process of encryption and compression

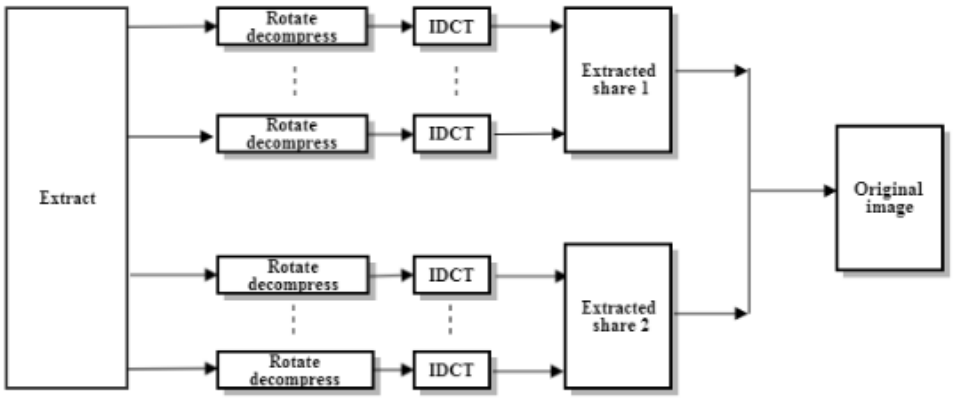


Fig.2. Receiver side process of decryption and decompression

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

IV. PROPOSED WORK

A. *Visual Cryptography Using Random Grids*

While the approach by Naor and Shamir [1] offers excellent security once one possesses solely one share, it suffers from the requirement to represent every pixel within the original image by multiple pixels in every share, leading to a decrypted image that's 2-4 times larger than the first image. This technique needs additional time to encrypt and decrypt images as well as to transfer encrypted images across a network.

A scheme was proposed by Kafri and Keren [3] that did not require the use of pixel expansion through the use of random grids (RG). RG scheme takes an input image and transforms it into multiple cipher-grids that give no information on the original image. However, RG schemes have the additional advantage that they require no pixel expansion, and thus each share and the resulting decrypted image retains the size of the original image. Kafri and Keren proposed three similar 2 out of 2 algorithms employing random grids in 1987. Qualitative testing disclosed that the first algorithm they present produces results superior to those produced by the others, so this formula is hand-picked for discussion.

Algorithm

Step 1: Generate R_1 as a random grid
Step 2: **for** (each pixel R_1 [x, y], $1 \leq x \leq w$ and $1 \leq y \leq h$) **do**
Step 3: R_1 [x, y] = rand_pixel (0, 1)
Step 4: **for** (each pixel B [x, y], $1 \leq x \leq w$ and $1 \leq y \leq h$) **do**
Step 5: {if (B[x, y] = 0) R_2[x, y] = R_1[x, y]
else R_2[x, y] = R_1[x, y]
}
Step 6: output (R_1, R_2)

Note that rand_pixel (0, 1) is a function that returns a binary 0 or 1 to represent an opaque or transparent pixel, respectively, by a coin coin-flip procedure. Here the initial grid R_1 is a combination of random collections of zeros and ones. Second grid R_2 is next generated based on the input image and R_1. This process occurs by scanning each pixel of the input image. If a pixel at location [x, y] in the input image is found to be white, then the pixel R_2[x, y] is set to be the same as R_1[x, y]. If, instead, the pixel at [x, y] in the input image is black, then the pixel R_2[x, y] is set to be the complement of R_1[x, y]. The decryption process takes place by superimposing the two random grids pixel by pixel using OR operation which is identical to that of Naor and Shamir's 2 of 2 algorithm.

B. *Transmitter Side Process*

1) *Encryption of Image Using Random Grid Technique*: The original image is encrypted by creating the random shares based on visual cryptography using random grids. Each share contains collection of random pixels. No single random share reveals the secret information.

2) *Discrete Cosine Transform:* Process the random share image in small blocks and apply two-dimensional discrete cosine transform to each block and we obtain DCT components of each block.

3) *Compression:* The share of the image to be placed in the cover image is compressed to be space efficient. In order to achieve objective, a lossy compression technique DCT is used for compressing the share. Lossy compression is a data encoding method which compresses data by discarding (losing) some unwanted portion of it.

In each block, most of DCT components have high energies in low frequency bands; we only require low frequency components. The low frequency components we can get through a simple low pass filter that is, left-up corners of each block with size of NC × NC are selected and higher frequency components are dropped. As a result of this process we can compress the transmitting images.

4) *Rotation and Embedding:* After the compression we have to rotate the each small block randomly, so as to make rotated DCT components be independent of each other. The compressed rotated image is covered by a random image and sends to Destination over a transmitting media.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

C. *Receiver Side Process*

1) *Extraction*: In order to extract the original image, authorized people receive the mixtures and turns back the rotated DCT components and using inverse discrete cosine transform (IDCT), so that the original images are decrypted.

2) *Inverse Rotation and Inverse Cosine transform:* The original image and random image should separated in order to reconstruct the original image. The rotated DCT components have to be restored. The receiver is beforehand given the rotation "key" by the transmitter. Using this rotation "key", the receiver can reconstruct the original images. Without rotation key, it is difficult to reconstruct the original DCT components. Finally the receiver can obtain the estimated original images from the observed mixtures by applying inverse discrete cosine transform (IDCT) to DCT components.

3) *Decryption of Image:* The shares and cover images are separated during extraction. The obtained shares are superimposed to get the original secret image.

Algorithms

Transmitter side algorithm: The transmitter side algorithm describes the encryption stages of the secret information as follows:

Algorithm 1

- Step1: Take an image as input.
- Step2: Encrypt the image by creating shares by the VC using random grid technique. Each share is treated as information.
- Step3: First divide the share (target image) into blocks.
- Step4: Apply DCT (Discrete Cosine Transformation) on each divided blocks.
- Step5: Then rotate the DCT blocks keep the direction of rotation as key for reconstructing the image.
- Step6: Then embed the share image with another random cover image.
- Step7: The random image is also divided into blocks and applies DCT on each block and the original image is covered by random image and it is send to the destination. This process is called embedding.

Receiver Side Algorithm: The Receiver side algorithm describes the decryption stages of the secret as information as follows.

Algorithm 2

- Step1: The random image is taken out. The share image or target image and random image are separated. This process is called extraction
- Step 2: The DCT blocks are reconstructed for the source image using the rotation key.
- Step 3: Then inverse DCT is applied to each block
- Step 4: The share image is reconstructed.
- Step 5: Finally the extracted shares are superimposed to get the original image.

V. SIMULATION RESULT

The simulation results are shown below. We have taken a 256×256 binary image as original image. Fig 1 shows the creation two shares using random grid technique. The sizes of the shares are same as that of the original image. Fig 2 shows the two compressed shares generated using DCT compression technique. Fig 3 shows the two 256×256 moon and clock cover images. Fig 4 shows the compressed cover images. Fig 5 shows the secret embedded cover images using lsb substitution. Fig 6 shows extracted decompressed shares from cover images. And finally the fig 7 shows original secret image obtained by overlapping both the shares. We can observe that the quality of the reconstructed image is not same as that of the original image because of the high compression ratio. The table 1 gives the PSNR of the compressed share image to compressed extracted image based on the number of LSB bits substituted in the cover

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

image. The PSNR of the original share image before compression to extracted final decompressed share image is 31.4756. The compression can be given by

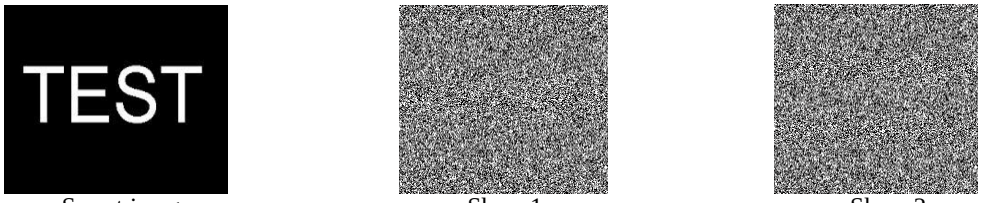
$$\text{Compression ratio}=\frac{\text{size of the original image}}{\text{size of the compressed image}}$$

We found that initial size of the share is 65KB and compressed share is 5KB. Hence compression ratio is 13.

No LSB bits substituted	PSNR of the share image to extracted image	MSE of the share image to extracted share image
1	2.8580	7.9097e+03
2	3.2306	1.9467e+03
3	9.3910	471.2605
4	15.6960	110.3464
5	22.3154	24.0339
6	29.6764	4.4128
7	39.2131	0.4910

Table.1. PSNR and MSE

A. *Encryption.*



Secret image Share 1 Share 2

Fig. 3 Encryption of secret information using Random Grid technique

Fig. 4 Compression of Shares using DCT

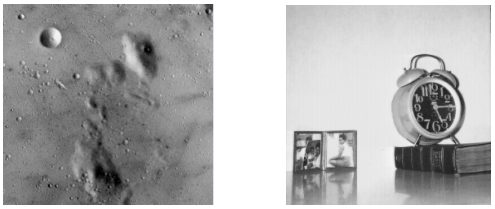


Fig. 5 Cover images to hide shares

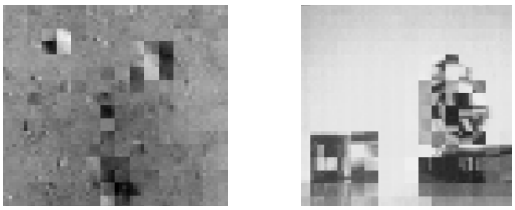


Fig. 6 Compression of cover images

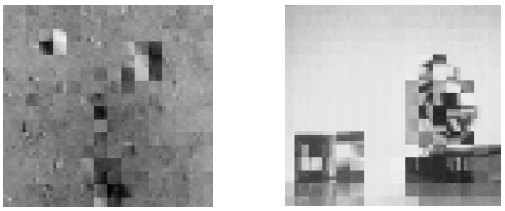


Fig. 7 Secret information embedded cover images

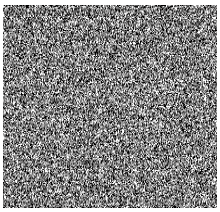
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

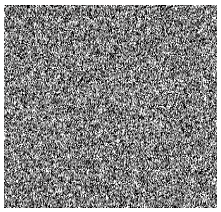
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

B. ***Decryption.***





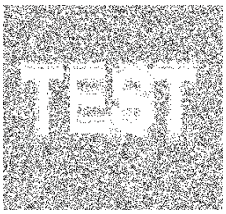


Fig. 8 Extracted secret shares from cover images

Fig. 9 Reconstructed secret image

VI. CONCLUSIONS AND FUTURE WORK

Visual cryptography is that current space of analysis wherever heap of scope exists. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. In the existing VC schemes no security is provided to the secret shares and intruder can alter its bit sequences to create fake shares. In this paper we proposed a steganography, visual secret sharing scheme and the combination of both. Therefore it provides higher levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways. And we proposed a new image compression and encryption technique based on Embedding and Discrete Cosine Transform (DCT).Binary secret shares are compressed using DCT. In the encryption process DCT blocks of transmitted shares rotated and covered with a random image to hide them. In the decryption process the covered binary secret shares can be extracted from the mixtures by applying extraction algorithm. Finally the original images can be reconstructed using rotation keys and inverse discrete cosine transform. This DCT based compression technique can also be applied to many VC schemes which suffer from huge share size problem. Therefore we can achieve a secure and fast image transmission. In this we have taken only binary image. The method can be applied to grayscale and binary images in the same way.

Our future works embody a safer secret writing technique with an alternate rotation technique and a reconstruction key. Additional advanced rotation manner makes it tougher for unauthorized individuals to reconstruct pictures without keys. Mean while the attention is given to improve the quality of the reconstructed image. Cryptography techniques like RSA, AES and hash functions can also be used with steganography to provide more security.

REFERENCES

1. M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology-EUROCRYPT ’94, LNCS 950, Springer-Verlag, pp. 1- 12,1995.
2. Ateniese G., Blundo C., De Santis A., and Stinson D. R., “Visual cryptography for general access structures,” Information and Computation, 129, 86-106, 1996.
3. O. Kafri and E. Keren, “Encryption of pictures and shapes by random grids,” Optics Letters, vol. 12, no. 6, pp. 377-379, June 1987.
4. S. J. Shyu, “Image encryption by random grids,” Pattern Recognition, vol.40, no. 3, pp. 1014-1031, 2007.
5. S. J. Shyu, “Image encryption by multiple random grids,” Pattern Recognition, vol. 42, no. 7, pp. 1582–1596, 2009
6. T. H. Chen and K. H. Tsao, “Visual secret sharing by random grids revisited,” Pattern Recognition, vol. 42, no. 9, pp. 2203-2217, 2009.
7. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Extended schemes for visual cryptography,” Theoretical Computer Science, vol.250, pp. 143-161, 2001
8. C. C. Chang, W. L. Tai, and C. C. Lin, “Hiding a secret color image in two color images,” Imaging Science Journal, vol. 53, no. 4, pp. 229–240,2005
9. C. C. Thien and J. C. Lin, “An image-sharing method with user-friendly shadow images,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 12, pp. 1161–1169, 2003.
10. Andrew B. Watson “Image Compression Using the Discrete Cosine Transform”, NASA Ames Research Center, Mathematica Journal, 4(1), p. 81-88,1994
11. A. Alfalou C. Brosseau, N. Abdallah, and M. Jridi,“Simultaneous fusion, compression, and encryption of multiple images”, OPTICS EXPRESS 24024Vol. 19, No. 24 OSA, 2011
12. Maher Jridi and Ayman AlFalou, “A VLSI Implementation of a New Simultaneous Images Compression and Encryption Method”, IEEE-978-1-4244-6494-4/10, 2010
13. Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban , Faculty of Information and Technology, Applied Science University, “Image Encryption Using DCT and Stream Cipher,” European Journal of Scientific Research, Vol.32, No.1 , pp.48-58,2009
14. Masanori Ito, Noboru Ohnishi, Ayman Alfalou and Ali Mansour, “New Image Encryption And Compression Method Based On Independent Component Analysis”, IEEE, 2007.