

An Improved Approach for Colour Extended Visual Cryptographic Scheme using ARTMAP Network

J. Ida Christy¹ and Dr. V. Seenivasagam²

*Associate Professor in CSE Dept.,¹
Unnamalai Institute of Technology, Kovilpatti, India
idaselvin@gmail.com
Professor in IT Dept.,²
National Engineering College, Kovilpatti, India
yespee1094@yahoo.com*

Abstract

Visual Cryptography is a powerful technique that combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be divided into shares that can be stacked together to approximately recover the original image. Extended Visual Cryptographic Scheme (EVCS) uses meaningful images to hide the shares of the secret image. In this paper, a new model of EVCS using ARTMAP network is presented that produces the shares with the same size as that of the original image. The results obtained are better than most existing schemes. The effectiveness of our scheme is demonstrated by real examples.

Key words: Extended Visual Cryptographic Scheme, Shares, ARTMAP network Secret sharing.

1. INTRODUCTION

TODAY'S computer and communication networks are becoming more and more dynamic, distributed, and heterogeneous, which, combined with the complexity of underlying computing and communication environments, increases significantly the security risk by making the network control and management much more challenging than ever.

Though the computer networks provide simple and inexpensive means of information exchange, they also expose the information to various types of threats. It is generally desired that the information being sent on computer networks is protected against eavesdropping and unauthorized modification.

Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography can be categorized into three different schemes: symmetric cryptography, asymmetric cryptography and secret sharing.

Symmetric-key systems use a single key that both the sender and the receiver have. Symmetric cryptography is susceptible to plain text attacks and linear cryptanalysis meaning that they are hackable and at times simple to decode. With careful planning of the coding and functions of the cryptographic process these threats can be greatly reduced. Asymmetric cryptography uses different encryption keys for encryption and decryption. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption. These keys are labelled or known as a public and a private key; in this instance the private key cannot be derived from the public key.

The original text, or *plaintext*, is converted into a coded equivalent called ciphertext via an encryption algorithm. Only those who possess a secret key can decipher (*decrypt*) the cipher text into plaintext.

The discipline that study techniques for deciphering cipher messages and detecting hidden messages is called *cryptanalysis*. It denotes the set of methods for obtaining the meaning of encrypted information.

In contrast to symmetric and asymmetric cryptography, secret sharing is based on the distribution of the secret information over several parties. Only if the required subset of parties put their information together the secret is revealed.

The disadvantage of traditional symmetric and asymmetric cryptographic schemes is that they require complex operational steps for the encryption as well as for decryption of information. For average and inexperienced users, these schemes are rarely convenient to employ. The major part of the disadvantage is computational overhead. There is no perfect encryption algorithm so far. So people who want more secure system are trying to make the encryption algorithm more complex so that no one can break the system. But complex encryption algorithm takes more time to encrypt a message as the complexity of the crypto system increases.

The location of the secret message is very obvious. This is the reason why an encrypted message can easily be targeted by attackers.

In 1994 Moni Naor and Adi Shamir combined the two mechanisms: secret sharing and traditional cryptography. They introduced a new concept named Visual Cryptography for the encryption and decryption of printed materials such as images or text. The new scheme requires no complex mathematical operations but only the human visual system for the deciphering of a given printed material. The concept relies on transparencies which exhibit a white noise when each transparency is considered separately. The transparencies consist of randomly located white and black pixels. When stacking these transparencies together, the secret image is revealed. The decryption is executed by the human visual system and only the ownership of all transparencies can reveal the secret.

The shares generated by the above method are meaningless and look like random dots. With such appearance, they make easy for the attackers to look into shares; whether or not the secrets can be easily cracked open, the looks of the

meaningless shares are already revealing the existence of secrets to attackers. When the shares produced are meaningful images, then the attackers cannot find the secret image. A visual cryptography that reveals the target image by stacking meaningful images is Extended Visual Cryptography (EVC).

Until now various techniques have been used in EVC. However, it is seen that machine learning techniques have not been used in EVC. Neural networks have found its applications in various fields of science and are effective machine learning tool. The advantage of Neural Network is that it is a powerful data-modelling tool, which has the ability to recognize patterns even if there is no functional relationship between input and output.

ANNs are processing devices (algorithms or actual hardware) that are loosely modelled after the neuronal structure of the mammalian cerebral cortex but on much smaller scales. A large ANN might have hundreds or thousands of processor units, whereas a mammalian brain has billions of neurons with a corresponding increase in magnitude of their overall interaction and emergent behaviour.

Neural networks are typically organized in layers. Layers are made up of a number of interconnected 'nodes' which contain an 'activation function'. Patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'. The hidden layers then link to an 'output layer' where the answer is output.

Most ANNs contain some form of 'learning rule' which modifies the weights of the connections according to the input patterns that it is presented with. In a sense, ANNs learn by example as do their biological counterparts. There are many different kinds of learning rules used by neural networks

Depending on the nature of the application and the strength of the internal data patterns you can generally expect a network to train quite well. This applies to problems where the relationships may be quite dynamic or non-linear. ANNs provide an analytical alternative to conventional techniques which are often limited by strict assumptions of normality, linearity, variable independence etc. Because an ANN can capture many kinds of relationships it allows the user to quickly and relatively easily model phenomena which otherwise may have been very difficult or impossible to explain otherwise.

The advantage of Neural Network is that it is a powerful data-modelling tool, which has the ability to recognize patterns even if there is no functional relationship between input and output. We have tried to explore the possibility of the use of Neural Network for EVC.

Back propagation network is very powerful in the sense that it can simulate any continuous function given a certain number of hidden neurons and a certain forms of activation functions. But training a Back Propagation Network is quite time consuming. It takes thousands of epochs for the network to reach the equilibrium and it is not guaranteed that it can always land at the global minimum.

Once a Back Propagation Network is trained, the number of hidden neurons and the weights are fixed. The network cannot learn from new patterns unless the network is re-trained from scratch. Thus we consider the Back Propagation Networks

don't have *plasticity*. Assuming that the number of hidden neurons can be kept constant, the plasticity problem can be solved by retraining the network on the new patterns using on-line learning rule. However it will cause the network to forget about old knowledge rapidly. We say that such algorithm is not *stable*. The contradiction between plasticity and stability and phenomenon is called *plasticity/stability dilemma*.

Adaptive Resonance Theory (ART) is a new type of neural network. It is designed by Grossberg in 1976 to solve *plasticity/stability dilemma*. The first version of ART, ART-1, proposed by Carpenter and Grossberg in 1987, is used to cluster binary data. Since then several variations of ART have been developed. The most important ones are: ART-2, an extension of ART-1, used to cluster analog data, ARTMAP, a supervised learning mechanism for binary data, and Fuzzy ARTMAP, a supervised learning algorithm for analog data.

ARTMAP performs incremental supervised learning of labeled patterns. ARTMAP contains a pair of ART modules, ART_a and ART_b. Patterns (without labels) are sent to ART_a and their labels are sent to ART_b. ART_a and ART_b are linked by an associative learning network and an internal controller that ensures system to operate in real time. If a prediction made by ART_a disconfirmed by ART_b, a mechanism called match tracking will be triggered. It increases the vigilance at ART_a, which leads to the selection of new candidate.

With these advantages, this paper proposes a new EVCS using ARTMAP network. This paper is organized as follows: Section II deals with the related works. The proposed method is described in Section III. Section IV gives the experimental results, followed by the discussion in Section V. This paper is concluded in Section VI

2. LITERATURE SURVEY

This section briefly gives the advances in the area of Visual cryptography.

In 1994, M. Naor and A. Shamir[12] suggested a cryptography method namely Visual Cryptography in which the secret image is encrypted into 2 shares of random binary pattern

Later in 1996, Extended Visual Cryptography that produces meaningful shares was developed by G. Ateniese, C. Blundo, A. de Santis, and D. Stinson[2]. In 2012 Shyong Jian Shyu and Hung-Wei Jiang suggested a method the used a region incrementing visual cryptographic scheme in which linear programming is used. Shyong Jian Shyu[15], in 2013 used a random grid structure for a general access structure. In 1997 E.R. Verheul and H.C.A. van Tilborg[18] developed a (k, n) -threshold color visual secret sharing scheme based on pixel expansion for p color images. Each pixel is expanded to p sections, and each section is divided into p sub pixels and can produce n shares with p sections. When the k shares are stacked together, the p -color secret image is revealed. In 2003, Y. C. Hou[7] developed a method in which the secret image is decomposed into three separate images that are respectively colored Cyan (C), Magenta (M) and Yellow (Y). Then the halftone technique is used to translate the three color images into halftone images. Finally, by combining the three halftone images, a color halftone image can be generated. The

color halftone image takes eight different colors to display: Cyan, Magenta, Yellow, Black, Red, Green, Blue and White.

All these above methods generated random shares which gave a clue to the hackers that there is a secret message.

So later in 1996, Extended Visual Cryptography that produces meaningful shares was given by G. Ateniese, C. Blundo, A. de Santis, and D. Stinson[2]. Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu[8] in 2008 developed a method that uses four main procedures. The first procedure is color halftone transformation, where the color image is transformed to a color halftone image. The second procedure, pixel extraction process, extracts pixels from the color halftone image. Third is the encoding process. To generate the shares, two $N \times N$ cover images are used to encode the $N \times N$ secret image and make two $2N \times 2N$ shares. Finally, during the decoding procedure, the secret image can be easily reconstructed by stacking the two shares. There are two coding tables referred to in the encoding procedure: Cover Coding Table (CCT) and Secret Coding Table (SCT). As the names suggest, CCT is responsible for the encoding of the cover image, and SCT, on the other hand, is used to encode the secret image. In 2010 Ms. Kiran Kumari and Prof Shalini Bhatia[11] developed a multi-pixel visual cryptographic scheme for colour images. It used a simple watermarking algorithm to produce two meaningful shares. The visual quality was improved by using filters. In 2011 Gopi Krishnan. S, Loganathan. D[6] proposed a method of extended visual cryptography where a color image to be protected and a binary image used as key to encrypt and decrypt are taken as input. A secret color image which needs to be communicated is decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images are converted into binary image, and finally the obtained binary images are encrypted using binary key image, called as share-1 to obtain binary cipher images. To encrypt Exclusive OR operation is done between binary key image and three half-tones of secret color image separately. These binary images are combined to obtain share-2. In decryption the shares are decrypted, then the recovered binary images are inverse halftoned and combined to get secret color image. Kai-Hui Lee and Pei-Ling Chiu[9], in 2012 gave a new EVCS method. This method consists of two phases. In the first phase, based on a given access structure, meaningless shares are constructed using an optimization technique and the construction for conventional VC schemes. In the second phase, cover images are added in each share directly by a stamping algorithm. Pixel expansion is reduced to some extent.

All of these existing systems have the drawback of pixel expansion. Further the size of the image gets doubled because of which memory space requirement is also more.

In order to overcome all these limitations, in this paper, an Extended Visual Cryptography Scheme using ARTMAP Network that produces the shares whose size is same as that of the original images is proposed.

3. PROPOSED METHOD

In this section a brief description of the proposed method is given.

Two color images are taken as cover images. One image is taken as secret image. All these three images should be of same size. The three images are given as input where the secret image is divided into two shares and it is embedded with the two cover images. The secret image gets totally hidden in the two cover images. The two cover images when overlapped show the original secret image. All the images are of the same size as the original images.

The whole procedure can be seen in the Figure 1.

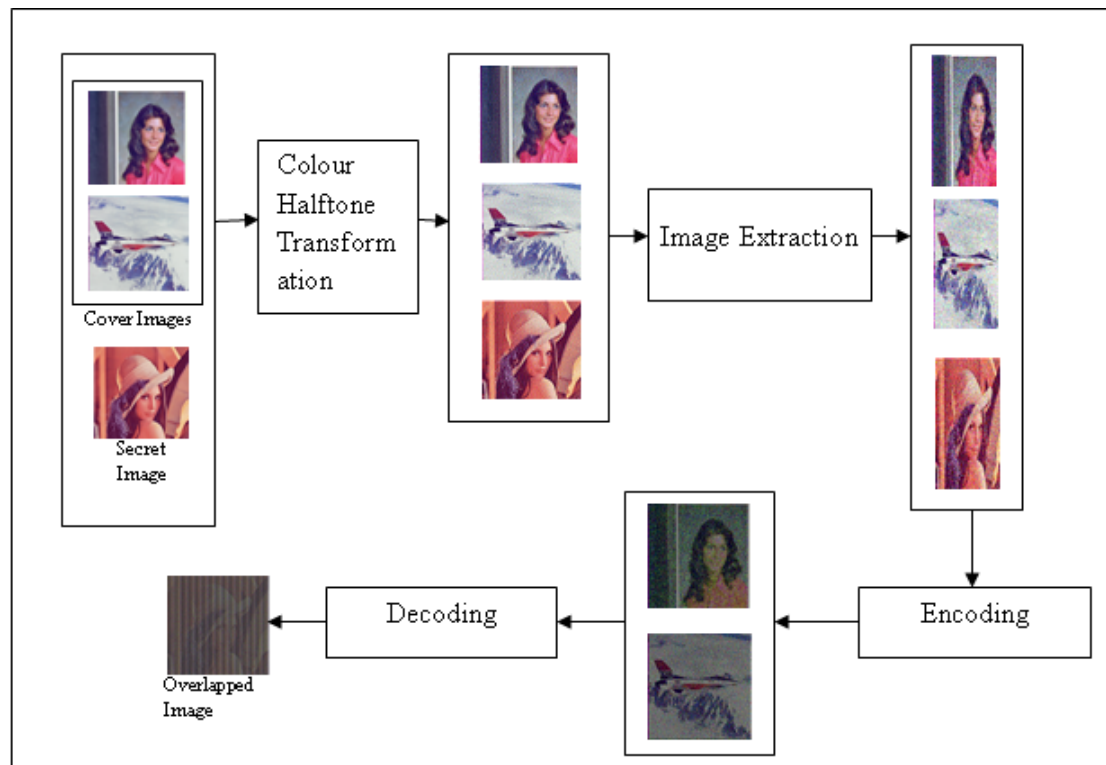


Figure 1 Block Diagram of the Proposed Method

The detailed description of every step is given below

3.1. Colour Halftone transformation

Colour halftone transformation is the first step that takes as input the cover images and secret image. All the three images are converted into halftone images. The images are converted into halftone images in three steps. They are

3.1.1. Image Resizing

The image is resized to half of its size. This is the step that aids in producing the overlapped image of the same size as that of original image. It also helps in reducing the memory capacity required for storing the image.

3.1.2. Colour decomposition

This is a pre-processing step for halftoning where the image is converted into monochrome images of cyan, magenta and yellow.

3.1.3. Halftoning

Halftoning is the reprographic technique that simulates continuous tone imagery through the use of dots, varying either in size, in shape or in spacing. Among the different halftoning techniques, Error diffusion technique is selected.

Error diffusion produces halftones of much higher quality than other techniques, with the trade-off of requiring more computation and memory. Error diffusion technique requires a neighbourhood operation and thresholding. The neighbourhood operation distributes the quantization error due to thresholding to the unhalftoned neighbours of the current pixel. The term "error diffusion" refers to the process of diffusing the quantization error along the path of the image scan. In the case of a raster scan, the quantization error diffuses across and down the image. Error diffusion accurately reproduces the gray level in a local region by driving the average error to zero through the use of feedback.

Halftoning is applied to all the three images.

3.2 Pixel Extraction

This step takes the halftone image as input. It is done to extract important pixel from the images. For this either the odd numbered rows or columns can be selected. In this method, odd numbered columns are selected. If the pixel size is 256, then the size of the extracted image is 128x256.

3.3. Encoding

In the encoding procedure the Secret Image is divided into two shares and the two shares are embedded in the two Cover Images namely Cover Image1 and Cover Image2. This step uses ARTMAP network to divide the Secret and the Cover Images into two shares. The encoding procedure is shown in Figure 2

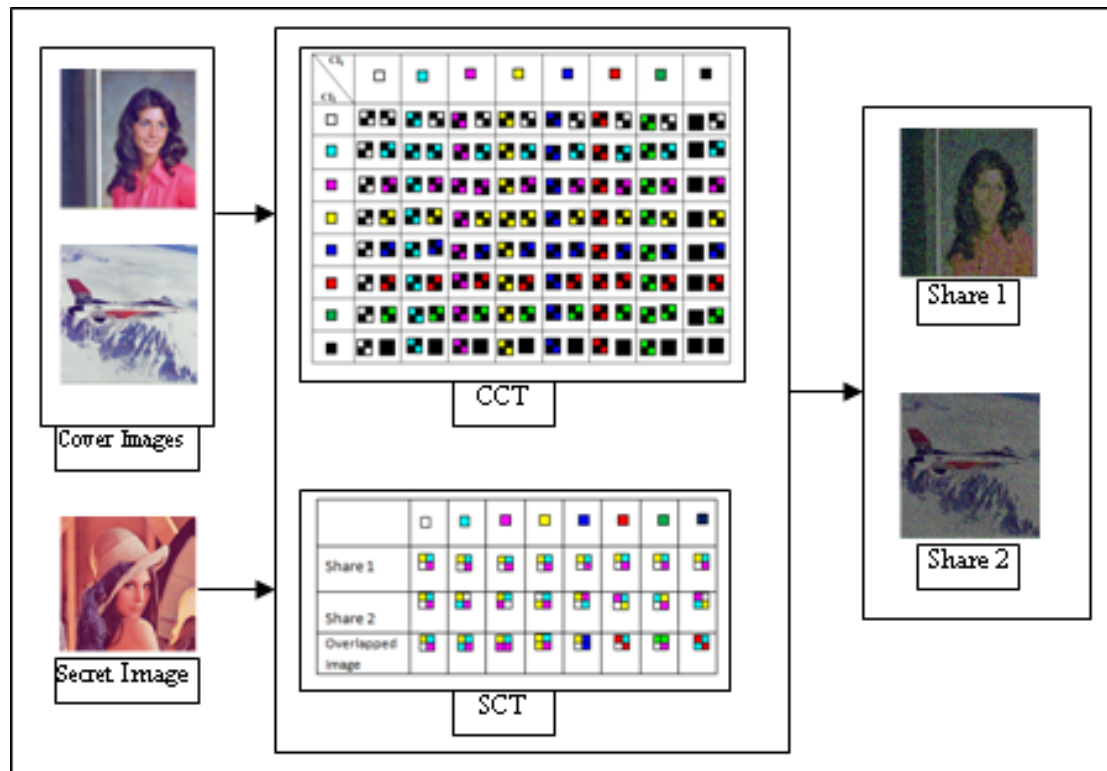


Figure 2 Encoding

































For the encoding procedure, two tables namely Cover Coding Table (CCT) and Secret Coding Table (SCT) are used.

There are three steps in encoding namely Secret Image Coding, Cover Image Coding and Share Production

3.3.1. Secret Image Coding:

The Secret Image is given as input. This Secret Image is coded with the Secret Coding Table (SCT). The SCT is used in the same way as it was used in Hou's second method as given in the Table 1. The ARTMAP network is first trained with this Secret Coding Table. The inputs to the ARTMAP network are the eight pixel values. The neural network is trained to produce the blocks of Share2 with four pixels namely Cyan, Magenta, Yellow and White. Once the network has been trained with the SCT, then it can be used to process the secret image. The pixel of the input image is given as input to the ARTMAP network. Then the ARTMAP gives the block for share2 as output.

Table 1 Secret Coding Table

								
Share 1								
Share 2								
Overlapped Image								

For each pixel of the secret image, the following process is done. First, for Share1, 2×2 block is built by permuting the four pixels *C*, *M*, *Y* and *W*. Then, the corresponding block for share2 is produced by the ARTMAP network. The input to the ARTMAP network is the pixel from the secret image. This pixel value is processed by the ARTMAP network and gives the corresponding block for share2.

















































































For example if the pixel in the secret image is green, Share1 gets a block with four pixels as Yellow, Cyan, White and Magenta. The ARTMAP network processes this pixel and the block in Share2 gets four pixels as Cyan, Yellow, White and Magenta. When all the pixels are processed, the two shares for the secret image are produced.

3.3.2. Cover Image Coding:

The two cover images namely Cover Image1 and Cover Image2 are given as input to the Cover Image Coding procedure. Cover Coding Table as given in Table 2 is used to code the cover image. This step generates two 2x2 blocks from the cover images. The ARTMAP network is trained to obtain the two blocks of pixel as given in Table 2.

The pixels of the Cover Image1 and Cover Image2 are given as input to the ARTMAP network. It produces two 2x2 blocks of pixels which becomes Share1 and Share2.

Table 2 Cover Coding Table

$CI_1 \backslash CI_2$								
								
								
								
								
								
								
								
								

3.3.3. Share Production:

The two shares produced in the secret image coding step and the blocks produced in the cover image coding step becomes the input for this step. The outputs are two patterns P1 and P2 with two regions R1 and R2. For example, when the pixel in Cover Image1 is Magenta and the pixel in Cover Image2 is cyan; two blocks (B1 and B2) are produced using Cover Coding Table. These two blocks are then combined with the two blocks (B3 and B4) produced from the secret image to form the two patterns (P1 and P2). This is done based on the position of the pixel in the shares. If the pixel belongs to an odd row, P1 has B1 and B3. Similarly P2 has B2 and B4. If the pixel belongs to even row, P1 has B3 and B1. Similarly P2 has B4 and B2.

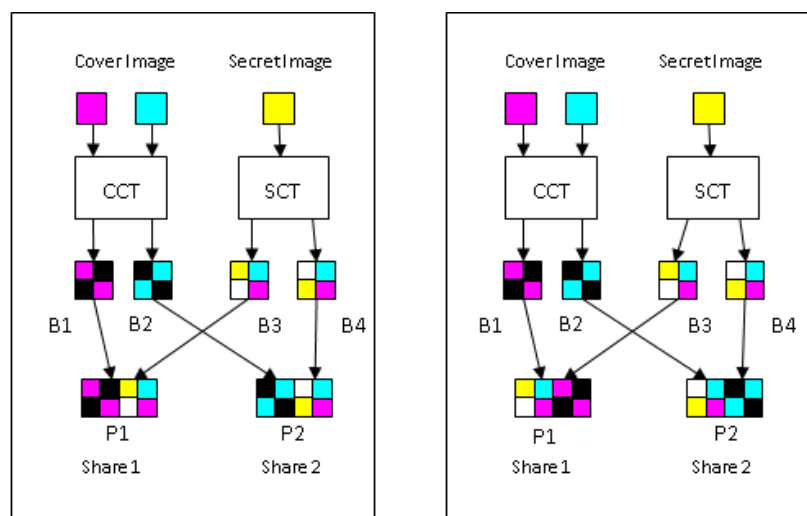


Figure 3 Production of shares for odd pixel and even pixel

The production of shares can be explained with the following steps:

```

CI1(i,j) – Pixel of the Cover Image1
CI2(i,j) – Pixel of the Cover Image2
SI(i,j) – Pixel of Secret Image
B1, B2 = CCT(CI1(i,j), CI2(i,j))
B3, B4=SCT(SI(i,j))
If CI1(i,j) & CI2(i,j) belong to odd row
    P1=B1+B3
    P2=B2+B4
Else
    P1=B3+B1
    P2=B4+B2
End if
End

```

Figure 4 Steps for production of shares

When all the blocks have been processed, the production of shares is completed. The complete share production process is shown in Figure 4.

3.4. DECODING

Decoding is the procedure in which the two shares are overlapped to produce the secret image. Some of the blocks become black after overlapping. However that does not affect the secret image. It improves the contrast of the secret image and makes the image clearer. The process of decoding a single pixel is shown in the Figure 5.



Figure 5 Decoding of a pixel

When the first block of Share 1 is overlapped with the first block of Share 2, it would produce a block consisting of black pixel. When the second block of Share 1 is overlapped with the second block of Share2 the pixel of the secret image is obtained. In this way, the whole secret image is obtained when the two shares are overlapped.

4. EXPERIMENTAL RESULTS

The input images of same size are taken. Cover Images are given as input to the ARTMAP network that produces two shares as output. Similarly the Secret Image is

given as input to the ARTMAP network which produces two shares as input. These shares are embedded with the shares of the Cover Images. The shares produced by this method are the meaningful images that do not give any idea about the secret image hidden in it. The secret image can be viewed at the decoding step by simply overlapping the two images. It does not need any mathematical calculations.

The Figure 6 shows the output obtained for three secret images namely Boat, Lena and Pepper of sizes 128x128, 256x256, 512x512 and 1024x1024. The input images and the secret images are of the same size. The Shares obtained are also of the same size. The overlapped image is also of the same size




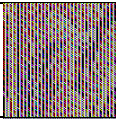
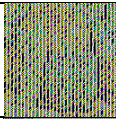
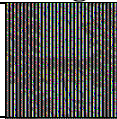








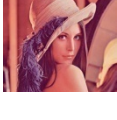
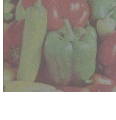
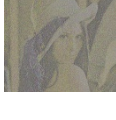
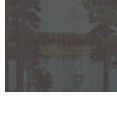
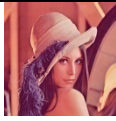


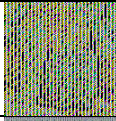
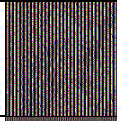







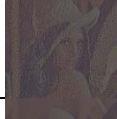


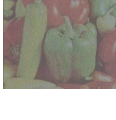

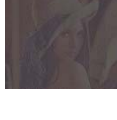

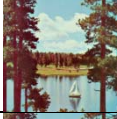
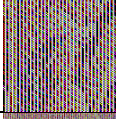
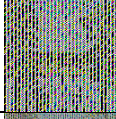
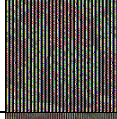


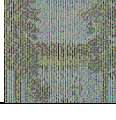

Secret Image	Cover Image1	Cover Image2	Size of the Images	Share1	Share2	Overlapped Image
			128x128			
			256x256			
			512x512			
			1024x1024			
			128x128			
			256x256			
			512x512			
			1024x1024			
			128x128			
			256x256			



Figure 6 5Share 1, Share 2, and Overlapped Image for the different Secret Image and Cover Images of 128x128, 256x256, 512x512, and 1024x1024

5. DISCUSSION

The probability of the secret image block being guessed correctly can be calculated by the formula $(1/p)^{N/2 \times N}$, where p is the number of block combination and $N/2 \times N$ is the size of the extracted secret image. If the pixel is blue, the block combinations that produce blue are 8. Hence the probability of the extracted secret image being guessed correctly is extremely low. This way, with each block randomly produced, our scheme makes it extremely difficult for an attacker to figure out what the secret image is.

PSNR and the time complexity are taken into consideration to analyse the performance of this method.

PSNR is the Peak Signal to Noise Ratio. The PSNR values of the images Boat, Lena, and Pepper of various sizes namely 128x128, 256x256, 512x512, 1024x1024 are calculated. It can be compared with the existing system as shown in the Table 3.

Table 3 PSNR Values for various image using ARTMAP network and Hsein Chu Wu et. al System

IMAGE	SIZE	PSNR Using ARTMAP(dB)	PSNR using Hsein Chu Wu et. al (dB)
Boat	128x128	41.1943	35.1727
	256x256	35.1681	29.1443
	512x512	29.1468	23.1260
	1024x1024	23.1260	17.1028
Lena	128x128	41.1914	35.1672
	256x256	35.1716	29.2290
	512x512	29.1479	23.1261
	1024x1024	23.1270	17.1035
Pepper	128x128	41.2727	35.2484
	256x256	35.2520	29.2290
	512x512	29.2350	23.2140
	1024x1024	23.214	17.1905

The graph showing the PSNR values of the three images of various sizes is shown in the Figure 7.

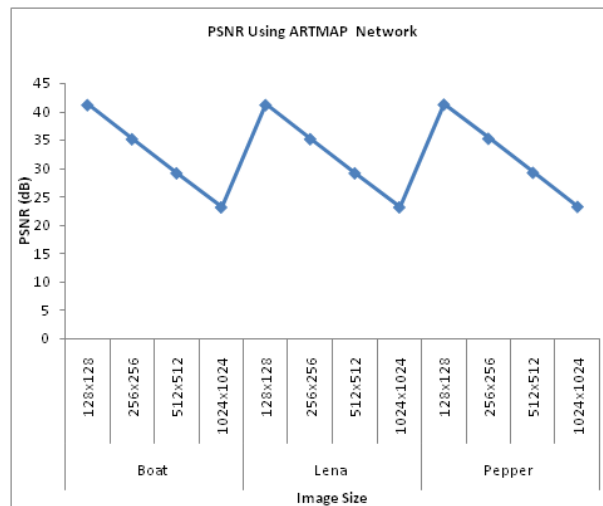


Figure 7 Graph Showing the PSNR values of different images

The comparison of the PSNR values of the existing system with the proposed system is shown in the Figure 8.

The next comparison with the existing systems is based on the memory space required for the overlapped image. This is shown in Table 4. From this table it can be observed that the memory space required for storing the overlapped image in the proposed system is less when compared to the existing system. The graph below in Figure 9 shows the comparison of the existing system with proposed system based on the memory space required to store the overlapped image.

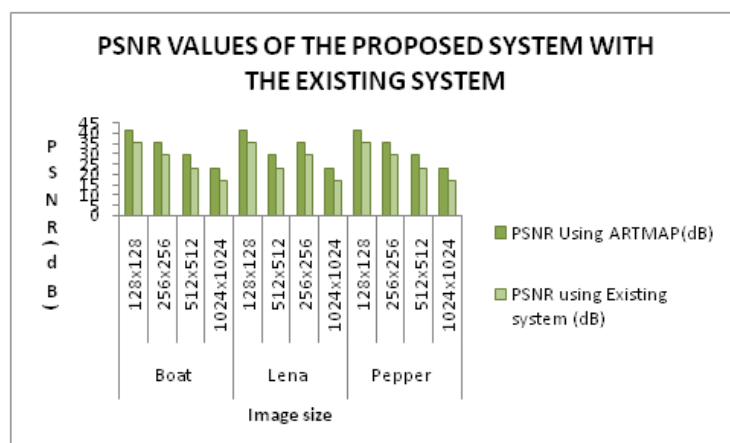
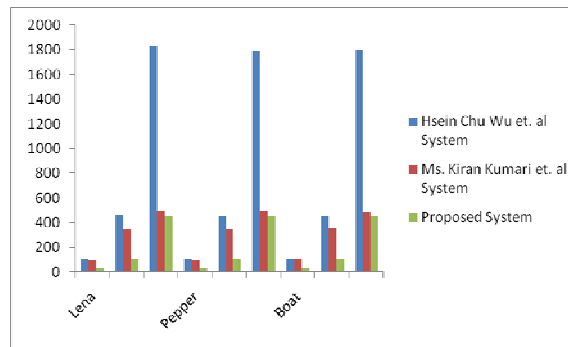


Figure 8 Graph showing the Comparison of proposed system with the existing system based on PSNR values

Table 4 Comparison of the proposed system with existing systems based on Memory space

Image	Memory Space Required for			
	Secret Image	Overlapped Image In		
		Hsein Chu Wu et. al System	Ms. Kiran Kumari et. al System	Proposed System
Boat	48.6KB	112	102	28
	193KB	450	356	112
	768KB	1802.24	490	450
Lena	48.6KB	114	100	28.7
	193KB	461	350	114
	768KB	1832.96	500	457
Pepper	48.6KB	112	100	27.9
	193KB	449	352	112
	768KB	1792	498	449

**Figure 9 Graph showing the comparison of proposed system with existing system based on memory space**

6. CONCLUSION

This paper suggests an efficient way to implement EVCS. It can be seen from the results that this method is of better performance than the existing systems. As ARTMAP network is used, image quality is better. The size of the overlapped image is same as that of the original image. The memory space required to store the original image is less.

This method can be enhanced to reduce the pixel expansion still.

REFERENCES

- 1) M.Amarnath Reddy, P.Shanthi Bala, G.Aghila , "Comparison of Visual Cryptographic schemes", International Journal of Engineering Science and Technology, Vol. 3, pp.4145-4150, 2011.

- 2) G. Ateniese, C. Blundo, A. de Santis, and D. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86-106, 1996.
- 3) Feng Liu, Chuankun Wu, Xijun Lin, "Step Construction of Visual Cryptography Schemes", *IEEE Transactions On Information Forensics And Security*, Vol. 5, 2010.
- 4) Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes", *IEEE Transactions on Information Forensics And Security*, Vol. 6, No. 2, June 2011.
- 5) Ge Song, Changgen Peng and Xuelan Miao, "Visual Cryptography Scheme Using Pi-sigma Neural Networks", *Proceedings of the 2008 International Symposium on Information Science and Engineering*, pp.679-682, 2008
- 6) Gopi Krishnan. S , Loganathan. D, "Color Image Cryptography Scheme Based on Visual Cryptography," *Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*, pp. 404-407, 2011
- 7) Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition*, Vol. 36, pp.1619-1629, 2003.
- 8) Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu, "Color Visual Cryptography Scheme Using Meaningful Shares", *Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications*, pp. 173-178, 2008.
- 9) Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures", *IEEE Transactions On Information Forensics And Security*, Vol. 7, No. 1, pp. 219-229 February 2012
- 10) InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee, "Color extended visual cryptography using error diffusion", *Proceedings of ICASSP 2009*, pp. 1473-1476, 2009.
- 11) Ms. Kiran Kumari, Prof. Shalini Bhatia, "Multi-pixel Visual Cryptography for color images with Meaningful Shares", *International Journal of Engineering Science and Technology*, Vol. 2, pp.2398-2407, 2010.
- 12) M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology – EUROCRYPT'94*, pp. 1-12, 1995.
- 13) T.Rajitha, Prof P.Pradeep Kumar, V.Laxmi "Construction of Extended Visual Cryptography Scheme for Secret Sharing", *International Journal of Computer Science and Network (IJCSN)* Volume 1, Issue 4, August 2012
- 14) P.S.Revenkar, Anisa Anjum, W .Z.Gandhare," Survey of Visual Cryptography Schemes", *International Journal of Security and Its Applications*, Vol.4,49-56,2010.
- 15) Shyong Jian Shyu, "Visual Cryptograms of Random Grids for General Access Structures", *IEEE Transactions On Circuits And Systems For Video Technology*, Vol. 23, No. 3, pp. 414-424, March 2013
- 16) Shyong Jian Shyu and Hung-Wei Jiang, "Efficient Construction for Region Incrementing Visual Cryptography" *IEEE Transactions On Circuits And Systems For Video Technology*, Vol. 22, No. 5, pp. 769-777, May 2012
- 17) S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, Vol. 39, pp. 866- 880, 2006.
- 18) E.R. Verheul and H.C.A. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes and Cryptography*, Vol. 11, No. 2, pp. 179-196, 1997.
- 19) C. N. Yang and C. S. Lai, "New colored visual secret sharing schemes," *Designs, Codes and Cryptography*, Vol. 20, No. 3, pp. 325-335, 2000.