ISSN:0975-9646

Security measures for Smart Devices through Cryptography Using Cellular Automaton

M.Venugopal[#1], Dr. E.G.Rajan[*2], Dr. Sharma[#3]

[#] *Dept. Of ECE, HIET, R.R.District*
[*]*President, Pentagram Research Center, Hyderabad.*
[*]Director, Adrin, Hyderabad.

***Abstract*— Present Embedded industry is emphasising more on Smart devices and they have gained much importance in daily life. The devices includes communication, Bio-Medical, image processing, Power, etc. While using smart devices (i-Button Technology) data acquisition and user authentication has to be done.Various security concepts are developed to suite these requirement. One such security measure is using cryptography. Cryptography has gained much importance in the recent past due to the advancement in the technology for securing information. Visual Cryptography is such a cryptographic technique through which users hide information securely based on key authentication. This paper examines a new approach in visual cryptography using pextral coding algorithm in the framework of cellular automata. Primarily a 3 x 3 matrix pextral icon is considered. A 2D pextral icon is a convex polygon formed of pixels in a nine neighbourhood enclosing the central pixel. This central pixel is similar to a pixel considered for an image in Cryptography. Dropping one, two or three pixels in the given matrix forms 16 convex polygons. Out of these 16 polygons, few will have mirror symmetry. Two such mirror symmetry polygons were considered and the central pixel of these polygons will form the image pixel. An algorithm is developed to generate two signatures on an ASCII image. Combining the two signatures will reconstruct the original image. Results show that no loss of information and improved security.**

***Keywords*— Visual Cryptography, Authentication, Key, Pextral Coding, ASCII Image.**

I. INTRODUCTION

With the advent of VLSI / Nano technology and the state of the art technology development, we have latest smart equipment available for use. At certain places the security aspect plays a major role. One of the security implementation and more useful method is cryptography. During the communication of plane text or image information between the source and destination cryptography is applied on data for security reasons. Cryptography uses the key matching for authentication purpose. It works on image or on plane text. One of the methods used to get the key and cipher is to incorporate nonlinearity in the plane text image. The smallest element of a digital image is pixel. The non linearity is achieved by pixel expansion. Where each pixel of a plane text image is expanded into a 2 or 4 sub pixels. The non linearity in an image or plane text secures the information from hacking/misuse. Visual cryptography is one of the cryptographic technique which allows visual information (Image, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. Image is a multimedia component sensed by human. Human visual system acts as an OR function. If two transparent objects are stacked together, the final stack of objects will be transparent. But if any of them is non-transparent, then the final stack of objects will be non-transparent. Like OR, 0 OR 0 = 0, considering 0 as transparent and 1 OR 0=1, 0 OR 1 =1, 1 OR 1=1, considering 1 as non-transparent. In k out of n visual cryptography scheme is a type of cryptographic technique where a digital image is divided into (n) number of shares by cryptographic computation. In the decryption process only k or more than k number of shares can reveal the original information [Here can form the original image]. Less than k number of shares can not reveal the original information. In Visual Cryptography algorithms a given image are plain text is divided into (n) number of shares where minimum k numbers of shares are sufficient to reconstruct the plain text image. In this paper we propose to use cellular automata of dimension 2 as graphic crypto systems i.e crypto systems to encrypt image define by pixels. These crypto systems have several differences compared to the visual schemes proposed to date. For this reason, we denote this cryptography as graphic cryptography. The proposal begins with a plane text message, uses a cellular automata algorithm of dimension 2 and ends with encrypted message which we call as cipher image and the decryption of original message back. The rest of this paper is organized as follows. Below visual cryptography is reviewed in order to compare the cellular automaton that we propose and visual one. Some definition and properties of cellular automata are presented in our proposal of a visual representation using cellular Automaton.Visual cellular automata is discussed in detail and we present conclusions.

II. RELATED WORK

Moni Naor and Adi Shamir [1] proposed a new scheme for decoding concealed images without using cryptography. Zhi Zhou et. al [2] proposed halftoning based visual cryptography by using void and cluster algorithm for encoding a secret image, achieved better performenace when compared to other traditional algorithms. A.Ross & A. Othman [3] explored the possibility of visual cryptography in biometrics. The technique was applied on different biometric entities and tested. Han Yanyan et. al [4] proposed a technique for visual secret sharing. A verifiable cryptographic scheme is proposed for verification of the shares and to authenticate and achieved an improvement in

security. L.J.Anbarasi et. al [5] shown that by stacking the halftone shares, shares, the first secret is revealed and when the second share is rotated to 180° and stacked to the first the second secret is retrieved which is of better quality.

Shyamalendu Kandar [6] have proposed a K-N secret sharing scheme for encryption using random number generator. The technique is said to have less mathematical calculations with other traditional techniques besides its high computational complexity. Sozan Abdulla [7] proposed a new cryptographic algorithm for color images by taking (n) pictures as input and generated n-1 images. Decoding is performed by selecting a subset of these n-1 images by placing them as a stack. The original image is same as that of the reconstructed image. Shyamalendu Kandar et. al [8] proposed a visual cryptographic scheme for color images by dividing the images into shares which are generated by using a random number and these shares are watermarked in invisible mode. The technique proved to have less mathematical calculation when compared to other schemes. Pavan Kumar Gupta et. al [9] proposed a variable length symmetric key based cryptographic scheme for color images based on secret key which is used for dividing the image into number of shares. Krishnan et. al [10] proposed a scheme for securing color images. The images are protected and for encryption as well as decryption a binary image is used as a key. Color space models are used for decomposition of the images. Such a scheme is proved to be efficient in communication of natural images across different channels. liu et. al [11] proposed a color visual cryptographic model of Naor and Shamir without any pixel expansion and termed it as (k,n)-VCS. Feng Liu [12] proposed an extended VCS by taking meaningful shares which are the random shares, termed it as embedded EVCS ad shown that the proposed system is competitive when compared to traditional techniques.

III. Problem Definition

Security aspect plays a major role in protecting the image or plane text information. Many schemes were developed to safe guard the image or plain text information. In certain security applications, a long key of 128/256 ASCII characters are divided into two keys. One of the keys is stored on client side and other on the server side. At the server, the two keys are combined to get the original key which authenticates the user. Visual cryptography uses the pixel expansion to divide a given image into number of shares. A combination of these shares will get back the original image. So the long key having ASCII characters are encrypted and decrypted to safe guard the information for better security. Various techniques are applied in visual encryption and decryption of plain text. PSNR of the output image will be less which is a setback in visual cryptography. For example, when we retrieve the image, a white gausion noise is being added in the image resulting in loss of contrast as white pixel is represented by light gray pixels and the black pixels represented by dark gray pixels. In Visual cryptography, Watermark technique is another technique applied for the purpose of security which employs Fourier transform. Because of the random patterns and secret sharing behaviour such a technique face problem in changing and removing the watermark.

IV. Proposed System

The proposed system overcomes the issues present in visual cryptography by considering a new approach "A Notion of pextral coding using cellular Automaton Algorithms". Visual cryptography uses each pixel of plane text image for example ASCII 'A' and expanded to four sub pixels. The same pixel expansion technique is applied in cellular automaton.

Visual Cryptography:

Visual Cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by Human Visual System (HVS). It is a kind of secret-sharing scheme that encrypts the secret image in to (n) number of shares. It is imperceptible to reveal the secret information unless a certain number of shares (k) or more are superimposed. As the decryption process is done by human visual system, secret information can be retrieved by anyone if the person gets at least k number of shares. The original schemes are 2 out of 2 scheme, (n) out of (n) schemes, k out of n schemes. In 2 out of 2 scheme method, the transparencies consisting of pixels are subdivided into 4 sub pixels. Black is opaque and the White is transparent. One pixel expanded into 4 sub pixels is termed as share. The 2 out of 2 scheme has 6 possible shares.

The 2 out of 2 scheme includes creation of transparencies. During creating transparencies, each pixel of secrete considered separately. The first transparency (Key) is created randomly and the second transparency (Cipher) is created depending on the key and the secrete. Initially the white pixels are constructed and the exact matching of pixels in both transparencies must be achieved. Again black pixels are constructed and complementary pixels in both transparencies must be matched. In N out N scheme, a secret is distributed over N transparencies and all (N) transparencies are required for decryption.

Pextral coding:

Using cellular automaton, the concept of pixel expansion is considered using pextral coding technique. Pextral coding uses a 3X3 cellular matrix as shown in the figure 1.

0 1 0
1 1 1
0 1 0

Figure 1: A 3X3 cellular matrix

In our proposed system an ASCII 'A' image is considered in a binary form as shown in the figure 2.

0 0 0 0 1 0 0 0 0
0 0 0 1 0 1 0 0 0
0 0 1 1 1 1 1 0 0
0 1 0 0 0 0 0 1 0
1 0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0 0

Figure 2: ASCII 'A' image in 9X6 cellular matrix

Cellular Automaton is 2-dimensional finite method (CA for short), A= (L; S; V; f) , is a 4-uplet, where L is the cellular space formed by a 2-dimensional array of size r _ s of identical objects called cells. The Pextral coding uses dropping of these cells in sequence as one, two or three cells to form 16 geometric patterns as shown in the figure 3.

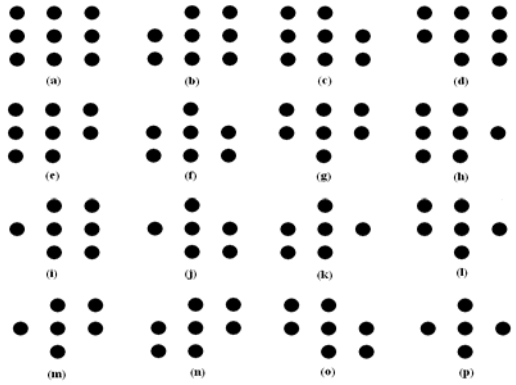

Figure 3: 16 Geometric patterns (Polygons)

Two geometric patterns out of these 16 patterns are considered as shown in the figure 4.(a) and (b)

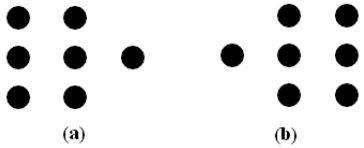

Figure 4: Geometric patterns with symmetry

The information in ASCII 'A' is in the form of pixels. Each pixel of this information is considered and expanded by the two geometric patterns by applying pixel expansion technique similar to visual cryptography to form signature 1 and signature 2 as shown in the figure 5. (a) and (b) respectively.

(a) (b)

Figure 5: Signature 1 and signature 2 for one pixel

This is the encryption technique we proposed in this paper. The decryption process uses these two signatures and combining of these signatures get back the original pixel information of the ASCII 'A'.

As shown in figure 6.

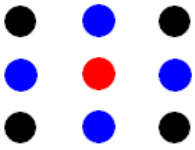

Figure 6: Original pixel retrieval after addition of signature1 and signature 2

For an ASCII 'A' image the initial pixel considered has co-ordinates as {(i,(j+3)}as shown in figure 7. Around this co-ordinate a cellular Automaton 3X3 matrix is shown in the figure separately with its own co-ordinates dropping two cells. The other co-ordinates are {(i-1),(j+3)},{(i-1),(j+2)},{(i),(j+3)},{(i),(j+2)}, (i+1),(j+2)}, {(i+1),(j+3)}, and {(i),(j+4)}.

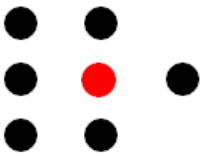

Figure 7: Initial pixel from ASCII 'A' representation

In these figure the pixel co-ordinate {(i-1),(j+4)} and {(i+1),(j+4)} are dropped and the remaining pixel information represents, the part of the signature one as shown in the figure 7 . Using this technique we consider the remaining pixels in ASCII 'A' as a centre pixel of 3X3 cellular matrix whose co-ordinates are {(i,(j+3)}. For all the pixels of ASCII 'A' the signature one is designed similarly as shown in the figure 7. Similarly dropping two pixels having co-ordinate {(i-1),(j+2)} and {(i+1),(j+2)}, the remaining pixel information represents the part of the signature two as shown in the figure 8. A similar technique is used by considering remaining pixels in ASCII 'A' as a centre pixel of 3X3 cellular matrix.

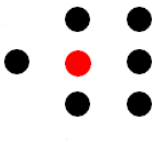

Figure 8: Signature 2 representation with the initial pixel from ASCII 'A'

The overall frame work of this proposal:

As shown in the figure 2: a 9X6 matrix is considered and ASCII is shown. To explain the Pextral coding algorithm, same is shown in figure 9.

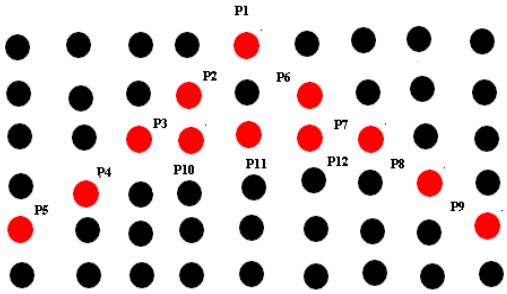

Figure 9: ASCII character 'A'

The ASCII character 'A' and its pixels are shown from P1to P12 in the figure 9..The co-ordinates are P1{(x,(y+4)}, P2{(x+1),(y+3)}, P3{(x+2),(y+2)}, P4{(x+3),(y+1)}, P5{(x+4),(y)}, P6{(x+1),(y+5)}, P7{(x+2),(y+6)}, P8{(x+3),(y+7)}, P9{(x+4),(y+8)}, P10{(x+2),(y+3)}, P11{(x+2),(y+4)}, P12{(x+2),(y+5)}. These pixels P1 to P12 forms the central pixel of the 3X3 cellular matrix. Applying this central pixels to the geometric patterns as shown in the figure 4 (a). Gives the signature 1. The signature 1 is shown in figure 10.

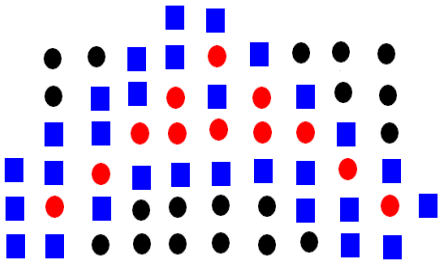

Figure 10. Signature 1

Similarly applying these pixels P1 to P2 to the geometric pattern as shown in the figure 4. (b). gives signature 2 as shown in the figure 11.

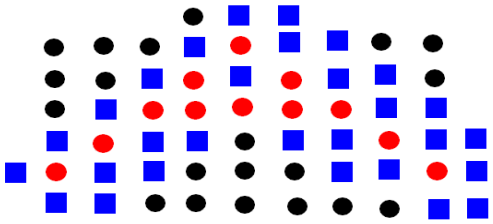

Figure 12. Signature 2.

The combination of signature1 and signature 2 gives back the original image as shown in the figure 9. In the signature 1 and signature 2 the blue pixels represents the new pixels during the expansion of the central pixels. Certain pixels will overlap during the expansion.

Pextral coding Algorithm:

1. Draw the alphabet 'A' black and white image
2. The height and width of the image should not exceed 160X160
3. Find the each pixel co-ordinate value of the alphabet 'A' and display them and also display the 'RGB' values of that pixel to form the above shape. The centre one is the original pixel
   Ex: original pixel (3,4)
4. The surrounding values of the original(central pixel) pixel (2,3),(2,4),(2,5),(3,3),(3,5),(4,4)
5. The original pixel has same value 'RGB' of the original pixel and the surrounding of the original pixel are not same.
6. Next create an image 2 with height and width above or equal to the original image.
   The height and width of the newly created image should not be less than to the original image
7. Send every original pixel of the alphabet 'A' and its surrounding six values to the newly created image 2 that form signature 1.
8. Create another image 3 with height and width above or equal to the original image
9. Again expand each pixel on the alphabet in another from as shown in figure 13

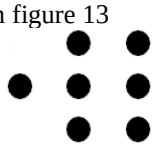

Figure: 13 Pixel expansion

10. Take the six adjacent neighbouring pixel values of the original signal to form the above shape, the centre one is original pixel.
    Ex: (3,4)
11. The surrounding values of the above original pixel are (2,4),(3,3),(3,5),(4,3),(4,4),(4,5)
12. Maintain the RGB values of the original pixel, its surrounding pixels are not same and every original pixel and its surrounding six values of the newly shaped format to the newly created image 3 that form the 'signature2'/
13. Create another image 4 and merge it with the pixel values of the image 2 and image 3 i.e signature 1 and signature 2 respectively.
14. Find the pixel 'RGB' values of the image 4. Compare these values with the original image pixel 'RGB' values. If the values are same then display them and ignore the remaining
15. The formed reconstructed image and the original image be same as shown in the figure14: Original image, figure 15: signatures 1&2, figure 16: reconstructed image.

Figure 14:

Figure 15:

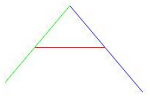

Figure 16:

V. Conclusions

A new approach called Pextral coding using cellular automaton is presented in this paper for encryption and decryption of an ASCII 'A'character. A pixel expansion technique similar to visual cryptography is considered and applied on cellular automaton using pextral coding method. Pixel information of ASCII 'A' is expanded and signatures are formed for encryption. Decryption method combines these signatures to form the original ASCII 'A' character. The original image and the Decrypted image are found to be same. An algorithm is developed to execute this process the output results are observed to see that the original image and the reconstructed image are same. The peak signal to noise ratio (PSNR) is determined and found to be infinite indicating the absence of white Gaussian noise in the process of encryption and decryption.

.

REFERENCES

[1] Moni Naor and Adi Shamir, Visual cryptography, Advances in Cryptology: EUROCRYPT '94 (Alfredo De Santis, ed.), Lecture Notes in Computer Science, vol. 950, Springer, 1995, pp. 1-12.

[2] Zhi Zhou, Arce, G.R. ; Di Crescenzo, G. , "Halftone visual cryptography", IEEE Transactions on Image Processing, Volume: 15 , Issue: 8, 2441- 2453, August 2006.

[3] Ross, A., Othman, A. , "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, Volume: 6 , Issue: 1, 70-81, March 2011.

[4] Han Yanyan, Yao Dong ; Cheng Xiaoni ; He Wencai , "VVCS: Verifiable Visual Cryptography Scheme", Seventh International Conference on Computational Intelligence and Security, 974- 977, 3-4 Dec. 2011.

[5] Anbarasi, L.J.; Vincent, M.J.; Mala, G.S.A., "A Novel Visual Secret Sharing Scheme for Multiple Secrets via Error Diffusion in Halftone Visual Cryptography", International Conference on Recent Trends in Information Technology, 129-133, 2011.

[6] Shyamalendu Kandar, "K-N Secret Sharing Visual Cryptography Scheme for Color Image Using Random Number", International Journal of Engineering Science and Technology, Vol. 3, No. 3, March 2011.

[7] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image", Journal of Computing, Vol.2, Issue 4, APRIL 2010.

[8] Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara, "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking" International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.

[9] Pavan Kumar Gupta, Naveen Hemrajani,Savita Shiwani, Ruchi Davey, "Halftone based Secret Sharing Visual Cryptographic Scheme for Color Image using Bit Analysis", International Journal of Computer Technology and Applciations, Vol 3 (1), 17-22, Jan-Feb 2012.

[10] Krishnan, G.S.Loganathan, D., "Color image cryptography scheme based on visual cryptography", International Conference on Signal Processing, Communication, Computing and Networking Technologies, 404-407, 21-22 July, 2011.

[11] Liu, F.,Wu, C.K. ; Lin, X.J., "Colour visual cryptography schemes" IET Information Security, Vol.2, Issue 4, 151-165, December 2008.

[12] Feng Liu, Chuankun Wu, "Embedded Extended Visual Cryptography Schemes", IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 2, 307-322, June 2011.