ENHANCED SECURITY SYSTEM USING SYMMETRIC ENCRYPTION AND VISUAL CRYPTOGRAPHY

Ranjan Kumar H S[1], Prasanna Kumar H R[1], Sudeepa K B[2] and Ganesh Aithal[2]
[1]Dept of CSE, NMAMIT, Nitte, Karnataka, India
[2]Dept of CSE, PACE, Mangalore, Karnataka India

ABSTRACT

With the rapid development of internet, transfer of data reliably and securely has become one of the challenges. In this paper we have introduced a novel visual cryptographic technique. This method is applicable for both Bitmap Color and Grayscale images. This method uses the concept of Residual Number System (RNS) based on Chinese Remainder Theorem (CRT) for share creation and share stacking of a given image. First, Secret image is hidden in cover image to get stego-image; a pixel (8 bit) of a Stego-image is taken and added with an eight bit key to get a cipher pixel. The algorithm used is additive mod 255.The key is generated using a pseudo random number generator and Mixed Key Generation technique. After encryption the cipher pixel is mapped into a Residue Number System of 'n' Shares. These 'n' Shares are stored or transmitted to the destination. The proposed approach like any other visual cryptographic approach is very secure, efficient, reliable, fast and easy to implement. Lastly, performance analysis of this visual cryptographic technique is done with respect to Histograms.

KEYWORDS: *Visual Cryptography, Sharing, Stacking, Residue Number System, Chinese Remainder Theorem, Mixed Key Generation.*

I. INTRODUCTION

Steganography is the science of hiding secret messages within a normal, innocent medium. Steganography has long been in use, even before the invention of the computer. For example, warring nations used invisible ink and microdots to communicate messages covertly. However, computer technology has taken steganography to the next level. Nowadays, messages are typically hidden within digital images, video and audio. This paper focuses on one particular popular technique, Least Significant Bit (LSB) Embedding, using digital images as the medium. The terminology is that a message is hidden within a cover image to produce a stego-image.

Visual cryptography can also be somewhat deceiving to the inexperienced eye, in such a way that, if an image share were to fall into the wrong hands, it would look like an image of random noise or bad art depending on the individual's experience.

It can be tempting to think of visual cryptography as a form of steganography, but it is important to understand the distinction between the two. In steganography, one seeks to conceal the existence of a message, perhaps by composing the message using invisible ink. By contrast, visual cryptography like its true cryptographic counterparts seeks only to conceal the message itself. It is, however, possible to combine steganography and visual cryptography to produce two benign-looking images that, when superimposed, reveal a third hidden image [1].The paper is divided into following sections. Section 1.1 1.2 and 1.3 gives the brief information about Visual Cryptographic Scheme (VCS), algorithms used in VCS and brief insight to image steganography. Section 2 describes the complete proposed security system. Section 3 gives the test results obtained. Section 4 gives the observations in terms of performance.

1.1 Visual Cryptography

Visual Cryptography is one of the cryptographic methods of sharing data but it is applied only for image format. Many works in this area have been done and several algorithms have been developed. In 1994 Naor and Shamir [2] Proposed VCS which is a simple and secure method that allows sharing of secret without the need of any cryptographic computations. To encode the image, original image is split into *n* modified versions referred as shares. Decoding can be done by simply stacking subset *s* of those *n* shares.

Figure 1 depicts the working of Visual Cryptography. This can be achieved by using any one of the following access structures [3]

I. (2, 2) VCS —this is a very simplest VCS scheme in which secret image is encrypted into 2 shares. To reveal the secret image 2 shares are overlaid or combined.

II. (2, *n*) VCS —this scheme encrypts the secret image into *n* shares such that when any two (or more) shares are overlaid the secret image is revealed.

III. *(n, n*) VCS —this scheme encrypts the secret image into *n* shares such that it can be revealed only when all *n* shares are overlaid.

IV. (*k*, *n*) VCS —this scheme encrypts the secret image into *n* shares such that when at least *k* shares are combined secret image can be revealed.

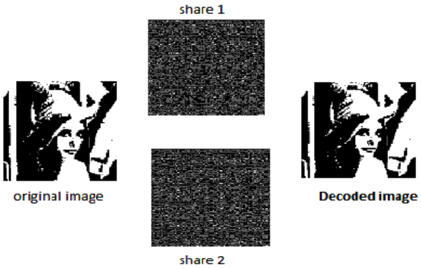

Figure 1: Basic VCS Scheme

1.2 VCS Algorithms

VCS Scheme normally involves two algorithms [4]:

- Algorithm for creating shares
- Algorithm for combining shares

VCS algorithm’s efficiency is very critical factor and reliability and level of security are some more metric which we need to consider while designing a VCS algorithm. The VCS system should be reliable enough such a way that intruders are not able to read the original image. One important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user.

1.2.1 Algorithm for creating shares:

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved.

1.2.2 Algorithm for combining shares:

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input.

1.3 Related Work

Recently so many researches in the field of visual cryptography have been done and so many scholars are working to improve VCS. Ming Sun Fu and Oscar C.Au [5] proposed about the process of using watermarking technique for visual cryptography. In this paper they have given an insight of how both halftone watermarking and visual cryptography may involve in securing secret image. Jaya, Siddhartha, Abhinav and Anjali [6] in their paper described about how authentication systems can be built using VCS. They also clearly explained how VCS and steganography can be combined to build a more secure system. Sagar kumar, Kamalendra varma, Rajasekhar chagati [7] proposed a color VCS using wavelet technique in which color image is converted to gray scale before applying VCS algorithm. Jagdeep varma and Vineeta khemchandani [8] proposed the authentication system using VCS and Watermarking. In this paper digital watermarking is used for providing the double security of image shares. Share embedding is done in frequency domain using Discrete Cosine Transform (DCT)

1.4 Image Steganography

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [9]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color [10]. These pixels are displayed horizontally row by row.

Image steganography is a method in which steganography technique is applied for images, which can be divided into two groups: those in the Image Domain and those in the Transform Domain [11]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [12].

1.4.1 Least Significant Bit Technique

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [12]. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [13]. For example a grid for 3 pixels of a 24-bit image can be as follows:

```
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)
```

When the number 200, which binary representation is `11001000`, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

```
(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)
```

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [13]

II. PROPOSED SYSTEM

The proposed security system first uses LSB technique to hide the secret image with the constraint that cover image is 8 times larger than secret image.

Visual Cryptography is a technique to make data secure. After dividing image into *'n'* shares, the individual shares are sent via different communication channels to destination such that intruder has less chance to get whole information. However the VCS's are not Perfect Secure System, because intruder may gain access to all communication channels and might retrieve all shares.

This paper proposes a solution for above security issue by encrypting the resulting Stego-image using symmetric encryption method before share creation. If intruder now gets all share, since Secret image itself is encrypted he or she might not get any of the information.

Our novel VCS technique is an *n* out of *n* approach in which a secret image after encryption by symmetric method is divided into '*n*' shares and in order to decrypt the secret image we must have '*n*' shares. Figure 2 gives the architecture of our approach.

First, for encryption additive modulo 255 algorithms is used. Keys are generated using a unique technique called Mixed Key Generation (MKG). In this method block of size of 8 byte keys are generated using PRN generation algorithm and individual bits from every byte is selected, since we have 8 byte word we can perform parallel operation with 8 byte of source data. Structure of Key generation technique is given in figure 3.By taking the keys generated by MKG method each pixel is encrypted to form Cipher pixel. Since, we can generate 8 keys at a time this improves the efficiency of cipher pixel generation.

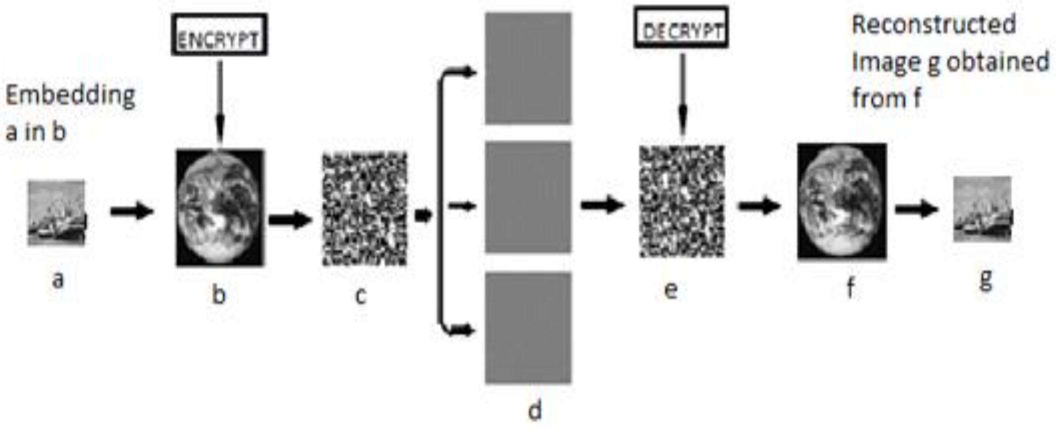

Figure 2: Proposed Architecture

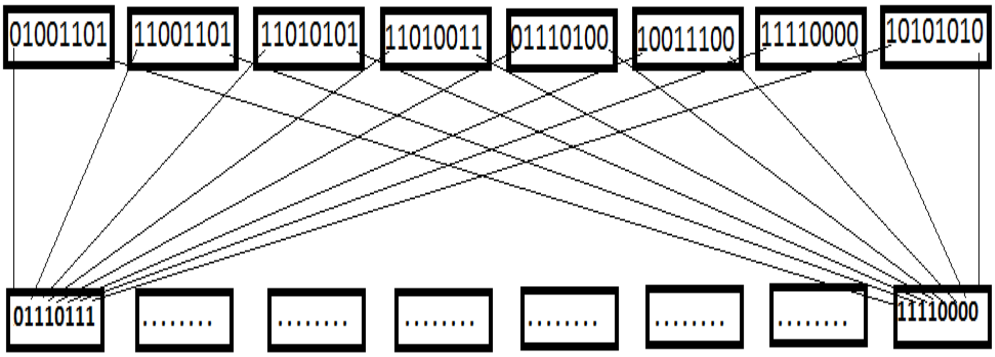

Figure 3: Key Generation

2.1 Share Creation Algorithm

RNS based on CRT concept is used for share creation. Although the proposed idea is n out of n approach we have generalized it to 3 out of 3 approach in which 3 shares are formed and all 3 shares are required to retrieve back original image. Chinese Remainder Theorem concept is used for share stacking. The share generation process is as given in figure 4.

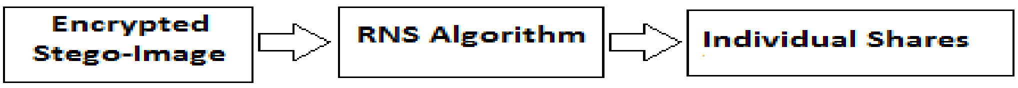

Figure 4: Share creation process.

The algorithm for the same is as given below:
Step 1 : select 3 prime numbers m1,m2,m3 such that their product is greater than 255 and gcd of selected 3 numbers is 1(i.e. relatively prime)
Step 2: calculate

$$r_{i1}\text{=X mod m1}$$

r_{i2}=X mod m2

r_{i3}=X mod m3

Where, r_{i1}, r_{i2}, r_{i3} are residues of *i* *'th* pixel; X is an individual pixel; m_1, m_2 and m_3 are selected prime numbers.

Step 3: Represent the residues r_{i1}, r_{i2}, r_{i3} as *i* *'th* pixel of share 1 2 and 3 respectively.

Step 4: Repeat step 2 and 3 until all pixels are processed.

2.1.1 An Example of share creation

For example consider a pixel value

X=128 and selected modulus m_1, m_2 and m_3 is 3, 5, and 17 respectively.

Applying above rule we get r_{i1}=1, r_{i2}=3 and r_{i3}=9.

So if the first pixel value of original image is 128 this value is mapped to 1 of first share, 4 of second share and 1 of third share respectively.

2.2 Share Stacking Algorithm

Chinese Remainder Theorem concept is used for share stacking process. The entire process is shown in figure 5

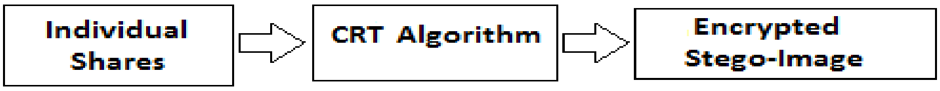

Figure 5: Share stacking process

Share stacking algorithm is given below:

Step 1: Calculate the dynamic range M=$m_1.m_2.m_3$

Step 2: Calculate A_i = M/m_i

Step 3: Find the solution of congruence's

$A_i.T_i$ mod m_i

Where T_i is multiplicative inverse of A_i

Step 4: We can get back original pixel by CRT using below equation

$$x = \sum_{i=1}^{N} A_i.T_i.r_i \bmod M$$

Step 5:Repeat step 4 until all pixels of shares are processed.

2.2.1 An Example of share stacking

Dynamic range M=3×5×17=255

A_1 = 255/3 = 85

A_2 = 255/5 = 51

A_3 = 255/17 = 15

Next we have to calculate inverse i.e

85 × 1 mod 3 = 1, so T_1=1

51×1 mod 5 = 1, so T_2=1

15×7 mod 17 = 1, so T_3=8

Using all these data we can get back original pixel *'x'*

x= (85×1×2 + 51×1×3 + 15×8×9) mod 255

= 1403 mod 255

x=128

III. Test Results

This security technique has been implemented using jdk.6.0_17 and we got following results:

3.1 Embedding Process:

Figure 6.a is selected as secret image and 6.b as cover image after embedding secret image in cover image using LSB technique we got figure 7.a as output. Since only some least significant bits are changed it cannot be identified by human eye.

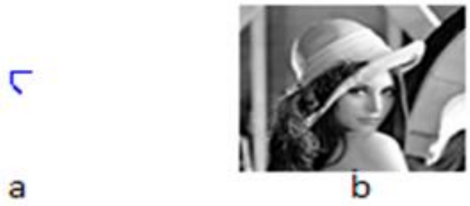

Figure 6: (a) Secret image (b) Cover image

3.2 Encryption Process:

Here numbers used as keys are generated using Pseudo Random Number generation algorithm; generated numbers are converted to binary representation in which 64 bits (8 bytes) binary is formed. One bit is selected from each byte to form 8 bit key using Mixed Key Generation (MKG) technique which is discussed in previous section. By using generated 8 bit keys using MKG algorithm, each pixel of stego- image is encrypted using additive modulo 255 algorithm. If there is 'n' number of pixels in stego-image than *'n'* different keys are used to encrypt each pixel. Here stego-image obtained is given as input to symmetric encryption algorithm and we got Figure 7.b as output. By comparing secret image and the encrypted image there is no visual information observed in the encrypted image.

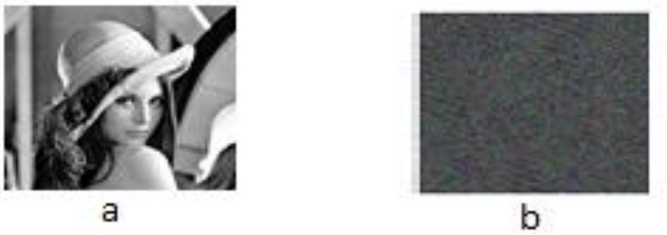

Figure 7: (a) Stego-image (b) Encrypted Image

3.3 Share creation Process:

Next the encrypted stego-image is selected and mapped into 3 shares using Share creation algorithm which is discussed in previous section. The resultant shares are as in figure 8; by observing the shares generated we can conclude that there is no pixel expansion problem which is solved compared to other visual cryptography techniques without using random grids and these individual shares are sent to destination via different communication channels. If intruder can access all of these communication channels than he may get all shares or subset of shares; since stego-image itself is encrypted even if he/she stack those shares they will get only random noise as reconstructed image. In traditional visual cryptographic technique if intruder can access individual communication channels by which shares are sent than he/she can construct original image very easily simply by stacking those individual shares; this problem is solved in proposed system. By these observations we can conclude that the proposed system has enhanced security, reliability, aspect ratio not distorted (i.e. no pixel expansion) and efficient.

Figure 8: Output of Share Creation Algorithm

3.4 Share stacking Process:

At destination share stacking algorithm given in table 2 is run. Input to this algorithm is shares which are generated as in figure 8 and we got Figure 9.a as output. This algorithm is exact reconstruction algorithm which does not have any data loss. This algorithm is very efficient which has less execution time.

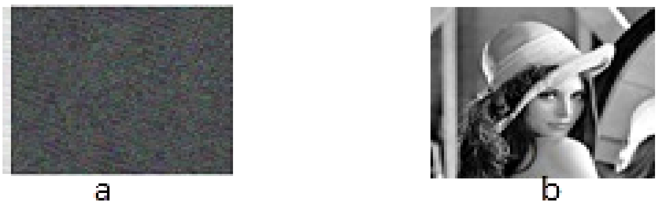

Figure 9: (a) Output of Stacking Algorithm (b) Reconstructed Stego- Image

3.5 Decryption Process:

Next we gave Figure 9.a as input to Symmetric decryption algorithm and we got Figure 9.b as output. Since the algorithm for initial used is based on feedback shift register same sequence of numbers are generated in destination also satisfying the requirement of symmetric key encryption.

3.6 Extraction Process:

Finally, Secret image is extracted from the stego-image which is as shown in figure 10.By Comparing Figure 6.a and Figure 10 we concluded that extracted image is exact copy of original image and there is no loss of information.

Figure 10: Extracted image

IV. PERFORMANCE ANALYSIS

The Histogram of original image and corresponding encrypted image is shown in figure 11 and figure 12. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the histogram of the original image. So, the encrypted image does not provide any clue to employ any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult. These properties tell that the proposed image encryption has high security against statistical attacks**.**

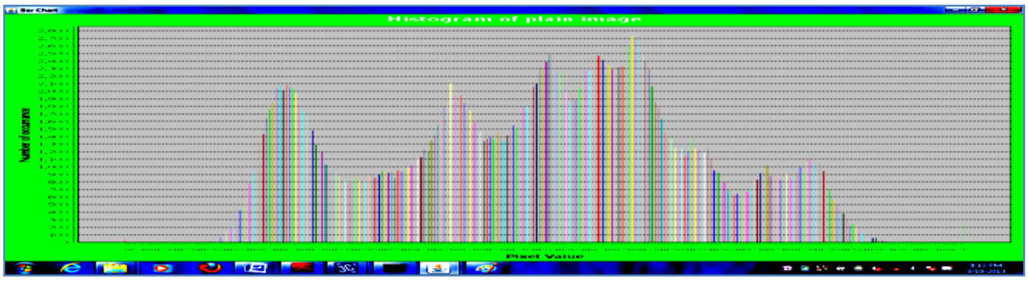

Figure 11: Histogram of Original image

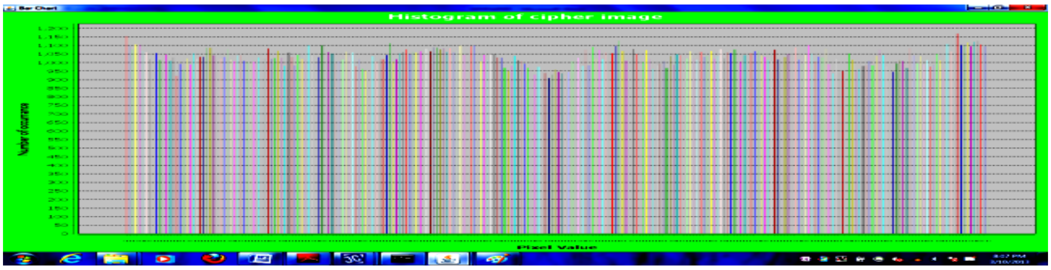

Figure 12: Histogram of Cipher image using MKG

V. CONCLUSION

We have introduced a new visual cryptographic technique. The traditional VCS suffer from pixel expansion problem. The proposed technique rectifies this problem. Another drawback of existing VC schemes is if intruder can access all communication channels than reconstruction of secret can be done easily; since symmetric encryption is introduced before sharing secret; our approach which overcomes this problem. The concept of symmetric encryption, steganography and Visual cryptography is combined in this paper to give a secured image sharing system. The performance analysis of MKG reveals that the proposed encryption method is ideal.

VI. FUTURE SCOPE

This paper contains some details about Visual Cryptography Scheme. If lossless Image compression methodology is applied before encryption we can strengthen cryptographic security. Because compressed image has less redundancy than the original image, cryptanalysis will be difficult [14].The proposed system can be extended such that it can be applied to all types of image formats like Jpeg, png…… etc. The LSB technique although it is simple and straight sometimes it is breakable so, in future any other steganographic which is not very easily breakable by intruder may be applied.

REFERENCES

[1]. Chang-Chou Lin and Wen-Hsiang Tsai. Secret image sharing with steganography and authentication. J. Syst. Soft., 73(3):405-414, 2004. ISSN 0164-1212.

[2]. A. Shamir and M. Naor,"Visual Cryptography," Advances in Cryptography -EUROCRYPT'94, Lecture Notes in Computer Science 950, 1995, pp. 1-12.

[3]. G. Ateniese, C. Blundo, A. De Santis, and D. R.Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129,No. 2, (1996), pp. 86-106

[4]. S.Manimurugan, K.Porkumaran "A New Fast and Efficient Visual Cryptographic Scheme with Forgery Detection" Proceedings of ICETECT 2011, pp. 594-599

[5]. Ming Sun Fu and Oscar C.Au, "Joint Visual Cryptography and Watermarking", 2004 IEEE International Conference on Multimedia and Expo (ICME), pp.975-978

[6]. Jaya, Siddhartha, Abhinav and Anjali, "Novel Authentication System Using Visual Cryptography", 2011 World Congress on Information and Communication Technologies, pp. 1181-1186.

[7]. Sagar kumar, Kamalendra varma, Rajasekhar chagati, “Securing Images Using Color Visual Cryptography and Wavelets”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3,pp.163-168, March 2012, ISSN: 2277 128X

[8]. Jagdeep varma and Vineeta khemchandani, “A Visual Cryptographic Technique to Secure Image Shares “,International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125, ISSN: 2248-9622

[9]. Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, *Computer Journal*, February 1998

[10]. “Reference guide: Graphics Technical Options and Decisions”,http://www.devx.com/projectcool/Article

[11]. Silman, J., “Steganography and Steganalysis: An Overview”, *SANS Institute*, 2001

[12]. Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, *Visual Image Signal Processing*, 147:03, June 2000

[13]. Krenn, R., “Steganography and Steganalysis”, http://www.krenn.nl/univ/cry/steg/article.pdf

[14]. William Stallings “Network Security and Essentials” Third edition 2009

AUTHOR’S BIOGRAPHY

Ranjan kumar H S received the Bachelor of Engineering Degree in Information science & Engineering from Visvesvaraya Technological University, Belgaum; Karnataka, India in 2008. He is currently working as Assistant Professor Grade at NMAMIT, Nitte. He is also pursuing his M.tech in part time basis at NMAMIT in department of CSE. He has 5 years of experience in teaching profession.

Prasanna Kumar H R working as Assistant Professor and HOD, Department of computer science at NMAMIT, Nitte, Karnataka, India. He completed his B.E in computer science and engineering in 1997 and M.tech in 2004. He has 15 years of teaching experience and his area of interest are Theory of computation,Cryptography,Design of Algorithms and Discrete Mathematics.

Sudeepa K B working as Assistant Professor in department of CSE in P.A.college of engineering,Mangalore,Karnataka,India.He completed his B.E in Visvesvaraya Technological University and M.tech in UVCE, Bangalore, India. He has 11 years of experience in teaching and his areas of interest are Database Management, Cryptography and UNIX.

Ganesh Aithal working as professor and Vice principal in P.A. college of engineering, Mangalore, Karnataka, India. He completed his B.E in Mysore University, M.tech in cochin University and Phd in NITK, Suratkal, Karnataka,India.He has 23 years of teaching experience. He has published many papers in National and International level.