A Novel Reversible Data Hiding Scheme that Provides Image Encryption

V. M. Manikandan and V. Masilamani
Indian Institute of Information Technology Design and Manufacturing Kancheepuram, Chennai-600127, India
Email: {coe14d001, masila}@iiitdm.ac.in

***Abstract*—Image encryption and reversible data hiding are two major areas of research in the field of information security. In this paper, we propose a new reversible data hiding scheme that provides an encrypted image as output, and which will be useful in secure medical image transmission. The novelty of the proposed scheme is that it generates an encrypted image as a by-product of reversible data hiding process. In the proposed scheme, the consecutive higher bit-planes having compression ratio less than 1 while using run-length coding with Elias-Gamma encoding scheme is considered. The compressed bits will be pseudo-randomly distributed in the same bit-plane, and the space created as a result of compression has been used to hide the secret message bits. Finally, the modified bit-planes are combined to generate the encrypted image. Experimental study shows that the proposed scheme outperforms the existing schemes in terms of embedding rate without compromising encryption efficiency.**

***Index Terms*—image encryption, reversible data hiding, run-length encoding, Elias-Gamma encoding, medical image transmission**

I. Introduction

In recent past, reversible data hiding schemes and image encryption techniques have been widely studied. Reversible data hiding schemes allow us to embed a secret message into an image. Later, the hidden message can be extracted along with the recovery of original image [1], [2]. The usefulness of reversible data hiding scheme is more in the applications like medical image transmission, military image transmission, etc., where permanent modifications on the original image are not acceptable. Image encryption is another active research area in which the original image will be converted into an incomprehensible form to protect the confidentiality of the digital content. In general, the encrypted image will have a noise-like or texture-like structure, and the authorized persons can recover the original image content [3].

In general, three parties are involved in a reversible data hiding scheme, they are the content owner, data hider, and data receiver. The content owner actually holds the digital content, and he/she wish to send this data to the data receiver in a secure way. The data hider is responsible for hiding additional secret message into the digital content for the purpose of data authentication or secret message communication. The data receiver is responsible for extraction of the hidden secret data from the received image along with the recovery of the original image. It should be noted that in some cases the same person may play multiple roles [4], [5]. For example in the case of cloud computing, the Cloud Service Provider (CSP) may do both data hiding and data extraction when CSP is using reversible data hiding scheme for the purpose of data coloring data coloring.

The existing reversible data hiding schemes explored the data hiding process in natural images [6]-[8] or in encrypted images [9]-[12]. In this paper, we propose a novel framework to generate an encrypted image as a by-product of reversible data hiding. The proposed scheme has achieved a very high embedding rate as compare to the well-known existing reversible data hiding schemes [9]-[11].

The proposed scheme will be useful for medical image transmission in telemedicine applications, where the medical images need to be transferred from one location to another in a secure way. In general, during transmission of medical images, the sender may have to send some more additional clinical information about the patient apart from the actual medical image. The new scheme allows to embed a large amount of secret data (i.e. clinical information) into an original image, and the resultant image will be an encrypted image (noise-like structure). The encrypted image ensures the confidentiality of the image content, and it is difficult for a third-party to estimate the actual image contents or the embedded secret data. At the receiver side, the extraction of secret data and recovery of the original image (image decryption) is possible. The receiver can use the recovered image and the extracted clinical data for further diagnosis. Usually, there will be a separate process for image encryption and another separate process for data hiding, but our proposed work achieves both in a single process.

II. Related Work

A detailed review of reversible data hiding schemes has been reported in [1], [2]. Some of the important reversible data hiding schemes for natural images are compression based reversible data hiding [13]-[15], difference expansion based reversible data hiding [16], and histogram shifting based reversible data hiding [6].

Manuscript received January 15, 2018; revised June 22, 2018.

doi: 10.18178/joig.6.1.64-68

Later, the difference expansion based reversible data hiding [17] and histogram shifting based reversible data hiding schemes [7] are efficiently modified by considering prediction errors from the image. Further, 2D prediction error histogram has been explored in [18]. Apart from this, an entirely different technique also has been used for reversible data hiding in [8], [19]-[23]. Reversible data hiding scheme for encrypted images include reversible data hiding by Reserving Room before Encryption (RRBE), and reversible data hiding by Reserving Room after Encryption (RRAE). In RRBE scheme, a vacant space will be created in the original image before encryption, and such spaces will be used to hide the secret message. But in RRAE scheme, the encrypted image pixel values will be modified to embed the secret data [24].

Many algorithms have been reported for image encryption, and a recent detailed review of image encryption technique is available in [3]. A few well-known recent image encryption algorithms have been reported in [21]-[23]. RC4 image encryption technique has been widely used for image encryption due to its balance between encryption/decryption time and security [24].

All the existing reversible data hiding schemes are concerned about the embedding of additional secret data into a natural image or into an encrypted image. Image encryption techniques tried to generate noise-like images from original images such a way that the original image cannot be obtained without additional security information. The novelty of the proposed scheme is that the encrypted image is generating as a by-product of reversible data hiding process.

III. Related Work

An overview of the proposed scheme is shown in Fig. 1. Algorithm 1 describes the proposed reversible data hiding procedure that provides an encrypted image as output. Algorithm 2 lists the sequence of operations required to be carried to recover the original image along with the extraction of the secret message bits from the encrypted image.

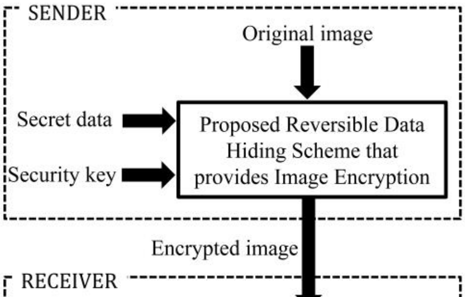
SENDER
Original image
Secret data
Security key
Proposed Reversible Data Hiding Scheme that provides Image Encryption
Encrypted image
RECEIVER
Security key
Proposed Data Extraction and Image Decryption Scheme
Secret data
Decrypted image

Figure 1. Overview of proposed reversible data hiding scheme

Algorithm 1 : Proposed reversible data hiding scheme that provides image encryption

```
Input   : Original 8-bit grayscale image $I$ of size $N×N$ pixels, secrete data bit sequence $S$ of length $M$, and security key $Y$.
Output  : Encrypted image $E$ of size $N×N$ pixels that contains secret data bit sequence $S$.
Step 1  : Apply bit-plane slicing on image $I$ to find all the different bit planes, say ($P_7$, $P_6$,..., $P_0$). Each bit-plane $P_i$ is a binary image of size $N×N$ bits, where $0\leq i\leq 7$.
Step 2  : Consider each of the bit-planes from $P_7$, $P_6$,...,$P_0$, and apply run-length encoding, say the resultant run-length sequence corresponds to each bit-planes are $R_7$, $R_6$,..., $R_0$
Step 3  : Apply Elias-Gamma encoding procedure on each of the sequence from $R_7$, $R_6$,..., $R_0$ to obtain an equivalent bit sequence representation, say the resultant sequences are $G_7$, $G_6$,...,$G_0$. Denote the total number of bits in each bit sequence from $G_7$, $G_6$,..., $G_0$ by $L_7$, $L_6$,..., $L_0$ respectively.
Step 4  : Find the compression ratio $C_i$ obtained from the bit-plane $P_i$ through Run-length encoding with Elias-Gamma encoding procedure as follows:
          $C_i = \frac{L_i}{N^2}$ , where $0\leq i\leq 7$
Step 5  : Find the smallest $k$, such that the compression ratio $C_i\geq 1$, $\forall i\geq k$, and $0\leq i\leq 7$
Step 6  : Find the number of bit-planes $K$ suited data hiding process, where $K$=8-$k$.
Step 7  : Convert the integer $K$ into a 3-bit binary representation, denoted by $B$.
Step 8  : Divide the secret message $D$ into $K$ blocks, say $B_1$, $B_2$,..., $B_K$, where the concatenation of $B_1$,$B_2$,...,$B_K$ will recover the secret message $D$, and $|B_i|=N^2-L_i$, $\forall$ $i$, $0\leq i\leq 6$, and $|B_7|= N^2-L_i-3$.
Step 9  : Find the bit sequence $T$ by concatenating $B$, $G_7$, $B_1$.
Step 10 : Initialize 8 binary matrices of size $N×N$ to keep the bit-planes corresponds to the final encrypted image, denoted by $U_7$, $U_6$,..., $U_0$
Step 11 : Find the most significant bit-plane $U_7$ by distributing the bits from $T$ in a pseudo-random locations of $U_7$ based on secret key $Y$.
Step 12 : Find $T_i$ by concatenating $G_i$ and $B_i$, where $i$=6, 5,... , $k$.
Step 13 : Find the new values of $U_i$ by distributing the bits from $T_i$ in a pseudo-random order based on security key $Y$.
Step 14 : Generate the final encrypted image $E$ which is embedded with secret data $D$ by combining the bit planes $U_7$, $U_6$,..., $U_k$ and $P_{k-1}$, $P_{k-2}$,..., $P_0$.
Step 15 : Output $E$
```

Algorithm 2 : Proposed data extraction and image recovery (decryption) scheme

```
Input   : Encrypted 8-bit grayscale image of $E$ of size $N×N$ pixels, and the security key $Y$.
```

Output : Recovered (decrypted) image I of size $N \times N$ pixels, and the extracted secret data bit sequence S.

Step 1 : Apply bit-plane slicing on image E to find all the different bit planes, say $E_7, E_6, \ldots, E_0$.

Step 2 : Generate a bit sequence T_7 by accessing bits from E_7 in a pseudo-random order based on the security key Y. Let us denote $T_7=(T_{70},T_{71}, T_{7N2-1})$.

Step 3 : Extract the first 3 bits from T_7, i.e. T_{70}, T_{71}, T_{72} and convert it into corresponding integer K.

Step 4 : Apply Elias-Gamma decoding procedure and run-length decoding procedure until getting a decompressed binary sequence of length N^2, say B. Let us assume that the Elias-Gamma decoded procedure considered the bits from T_{73} to T_{7q} for some q to generate a decompressed sequence of length N^2.

Step 5 : Generate the decrypted most significant bit-plane of recovered image P_7 by converting B into a binary matrix of size $N \times N$

Step 6 : Find the last bit-plane number k with hidden data

Step 7 : Access the bits from each bit-plane E_j to (in a pseudo-random order based on security key Y) find a corresponding bit sequence T_j, where j=6, 5,.., k.

Step 8 : Apply Elias-Gamma decoding procedure on T_j, until getting a binary sequence B_j of length N^2. Let us assume T_{jq} is the last element accessed in T_j to get B_j, where $j=6, 5, \ldots, k$, $0 \leq q \leq N^2$.

Step 9 : Convert B_j into a corresponding binary matrix P_j of size $N \times N$ as the recovered bit plane of decrypted image I, where $j=6, 5, \ldots, k$.

Step 10 : Find the extracted secret message S by concatenating the remaining bits (except the bits used to recover P_i) from T_i, where $i=7, 6, \ldots, k$.

Step 11 : Recover the original image I by combining all the 8 different bit-planes $P_7, P_6, \ldots, P_0$.

Step 12 : Output I, S.

IV. Experimental Study and Result Analysis

During experimental study, all the randomly selected medical images from Osrix medical image dataset have been converted into 8-bit grayscale images of size 512×512 pixels. The algorithms have been implemented and tested using Matlab2017a in a workstation having 32 GB RAM with Intel(R) Xeon(R) CPU of 3.46 GHz. The efficiency of the proposed data hiding scheme has been compared with existing reversible data hiding schemes in [9], [10], [25]-[28], and the efficiency of image encryption has been compared with RC4 image encryption scheme [24].

Efficiency of the proposed reversible watermarking scheme that provides encryption has been evaluated using embedding rate, recovery capability of original image from encrypted image, time complexity, encryption efficiency measures, and the security analysis.

A. Embedding Rate

Embedding rate (E) of data hiding scheme is defined as follows:

$$E = \frac{N_E}{N_T} \tag{1}$$

where N_E is the total number of bits that can be embedded into the image, and N_T is the total number of pixels in the original image. In general, embedding rate is measured by bits per pixels (bpp). Table I shows the comparison of embedding rate obtained from proposed scheme.

TABLE I. Comparison of Average Embedding Rate (in BPP)

Data hiding schemes	Embedding rate
Scheme in [9]	0.00097
Scheme in [10]	0.00390
Scheme in [28]	0.00390
Proposed Scheme	0.33294

Results from Table I show that in terms of embedding rate the proposed scheme outperforms the existing schemes [9], [10], [28].

The embedding rate of the proposed scheme is dependent on the amount of compression ratio that can be achieved from each bit-plane. While using run-length encoding scheme for compression, the compression ratio is purely dependent on the correlation between adjacent bits of a bit-plane. The correlation of adjacent pixels is defined below:

$$\frac{\sum_{i=0}^{N-1}\sum_{i=0}^{N-2} P(i,j)P(i,j+1)}{\sqrt{\sum_{i=0}^{N-1}\sum_{j=0}^{N-2} P(i,j)^2}\sqrt{\sum_{i=0}^{N-1}\sum_{j=0}^{N-2} P(i,j+1)^2}} \tag{2}$$

The average correlation value obtained from each bit-plane of the images is shown in Fig. 2. It can be observed that higher bit-planes are more correlated, and therefore more compression can be achieved from higher bit-planes.

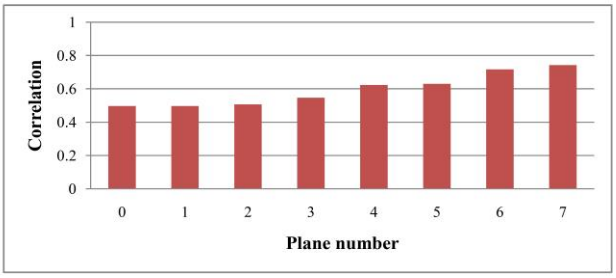

Figure 2. Correlation between adjacent pixels in each bit-plane

B. Recovery Capability of the Original Image

As per the proposed scheme, the original image can be recovered as it is from the encrypted image. Basically, the original image bit-plane has been compressed using run-length encoding with the help of Elias-Gamma encoding scheme, which is a lossless compression scheme. The vacant space created after compression has been used for the data hiding process. Therefore, recovery of original bit-plane and reconstruction of original image is possible.

C. Theoretical Time Complexity and Average Execution Time Analysis

Let us assume that original image has $N\times N$ pixels. The major operations in the proposed reversible data hiding scheme are run-length encoding on a bit-plane, Elias gamma code generation from run-length encoded sequence, and finally redistribution of pixels along with secret message to generate the new bit-plane of the encrypted image. Number of these operations are O(N^2) which is linear in input size. Image recovery and secret data extraction operation involves Elias-Gamma decoding procedure, run-length decoding procedure, and redistribution of decompressed bit sequence to recover the original bit-plane. No of these operations are also O(N^2). Table II shows the comparison between time complexity of the proposed scheme with the existing schemes [9], [10], [28].

TABLE II. COMPARISON OF THEORETICAL TIME COMPLEXITY

Data hiding schemes	Data hiding algorithm	Image recovery and data extraction algorithm
Scheme in [9]	O(N^2)	O(N^2)
Scheme in [10]	O(N^2)	O(N^2)
Scheme in [28]	O(N^2)	O(N^2)
Proposed Scheme	O(N^2)	O(N^2)

The practical usage of the proposed scheme is highly relied on the execution time required for the proposed scheme. It is observed that for data hiding process the proposed scheme is taking an average time of 16.038 seconds, and for image recovery process it takes 49.511 seconds.

D. Analysis of Proposed Encryption Scheme

An original medical image, and the corresponding encrypted image obtained from proposed scheme is shown Fig. 3. Efficiency of an encryption scheme can be evaluated by different measures. A few common measures used in our experimental study are Maximum Deviation (MD), entropy (E), number of pixel change rate (NPCR), and Unified Average Change in Intensity (UACI) [29], [30]. The comparison of efficiency measure obtained from the proposed scheme and the existing RC4 image encryption [24] is shown in Table III. Results represented in Table III show that the existing scheme [24] outperforms the proposed scheme with respect to three parameters MD, E, and NPCR. Although the proposed scheme outperformed by the competing method in three parameters (except UACI), the proposed method uses only one procedure to meet two objectives namely data hiding and image encryption. It should be noted that the proposed outperforms the competing schemes [9], [10], [28] while considering the embedding rate.

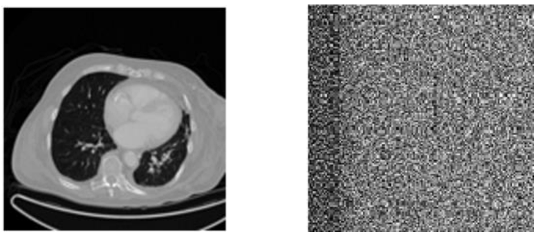
(a) Original image (b) Encrypted image

Figure 3. Sample results obtained during experimental study

TABLE III. COMPARISON OF ENCRYPTION EFFICIENCY PARAMETERS

Parameter	Scheme in [24]	Proposed scheme
Maximum deviation (MD)	**270371**	263941
Entropy (E)	**7.999**	7.973
Number of pixel change rate (NPCR)	**100**	95.024
Unified average change in intensity (UACI)	19.275	**22.235**

E. Security Analysis

As per the proposed scheme, the security key determines the pseudo-random locations to redistribute the compressed bit sequence and the secret message bits in a specific bit-plane. A determined adversary can attempt to recover the original image and secret data from the encrypted image by brute force attack only. Let us assume that there are M pixels are in the original image, where $M=N\times N$. In this regard, the possible number of pseudo-random sequences to recover original image is

$$\prod_{i=0}^{7}\sum_{x_i=1}^{M}\binom{M}{x_i} \tag{3}$$

where x_i indicates the possible number of bits that can be obtained during bit-plane compression. Equation (3) says that the choices to get exact sequence without security key is exponential, therefore the proposed cryptosystem is hard to break.

V. CONCLUSION

In this paper, we proposed a new reversible data hiding scheme that provides the encrypted image as output. The proposed scheme will be very much useful in the secure transmission of medical images in telemedicine applications. Experimental study of the proposed scheme on standard medical images from Osirix data set shows that the proposed scheme outperforms the existing reversible data hiding schemes in terms of embedding rate without compromising the efficiency parameters of image encryption. The proposed scheme is unstable against noises, and it can be improved in future by considering stable lossless compression schemes for bit-plane compression.

REFERENCES

[1] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, “A recent survey of reversible watermarking techniques,” *Information Sciences*, vol. 279, pp. 251–272, 2014.

[2] X. Li, W. Zhang, B. Ou, and B. Yang, “A brief review on reversible data hiding: Current techniques and future prospects,” in *Proc. IEEE China Summit International Conference on Signal and Information Processing*, 2014, pp. 426–430.

[3] M. Khan and T. Shah, “A literature review on image encryption techniques,” *3D Research*, vol. 5, no. 4, p. 29, 2014.

[4] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[5] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[6] W. L. Tai, C. M. Yeh, and C. C. Chang, “Reversible data hiding based on histogram modification of pixel differences,” *IEEE Transactions on Circuits and Systems for Video technology*, vol. 19, no. 6, pp. 906–910, 2009.

[7] D. S. Fu, Z. J. Jing, S. G. Zhao, and J. Fan, “Reversible data hiding based on prediction-error histogram shifting and EMD mechanism,” *International Journal of Electronics and Communications*, vol. 68, no. 10, pp. 933–943, 2014.

[8] T. S. Nguyen and C. C. Chang, “A reversible data hiding scheme based on the sudoku technique,” *Displays*, vol. 39, pp. 109–116, 2015.

[9] X. Zhang, “Reversible data hiding in encrypted image,” *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[10] W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[11] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[12] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[13] Z. Qian, X. Zhang, and S. Wang, “Reversible data hiding in encrypted jpeg bitstream,” *IEEE Transactions on Multimedia*, vol. 16, no. 5, pp. 1486–1491, 2014.

[14] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-lsb data embedding,” *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[15] N. A. Memon, “A novel reversible watermarking method based on adaptive thresholding and companding technique,” *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 5, no. 7, pp. 738–742, 2011.

[16] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[17] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” *IEEE Transactions on Image Processing*, vol. 20, no. 12, pp. 3524–3533, 2011.

[18] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, “Pairwise prediction-error expansion for efficient reversible data hiding,” *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013.

[19] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, “Hiding clinical information in medical images: A new high capacity and reversible data hiding technique,” *Journal of Biomedical Informatics*, vol. 66, pp. 214–230, 2017.

[20] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

[21] Y. Wang, K. W. Wong, X. Liao, and G. Chen, “A new chaos-based fast image encryption algorithm,” *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.

[22] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation,” *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[23] X. Wang, L. Teng, and X. Qin, “A novel colour image encryption algorithm based on chaos,” *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[24] A. Mousa and A. Hamad, “Evaluation of the rc4 algorithm for data encryption,” *International Journal of Computer Science and Applications*, vol. 3, no. 2, pp. 44–56, 2006.

[25] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Prentice Hall, 2002.

[26] P. Elias, “Universal codeword sets and representations of the integers,” *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 194–203, 1975.

[27] Osirix dicom image library. [Online]. Available: http://www.osirix-viewer.com/resources/dicom-image-library

[28] S. Agrawal and M. Kumar, “Mean value based reversible data hiding in encrypted images,” *Optik-International Journal for Light and Electron Optics*, vol. 130, pp. 922–934, 2017.

[29] J. Ahmad and F. Ahmed, “Efficiency analysis and security evaluation of image encryption schemes,” *Computing*, vol. 23, p. 25, 2010.

[30] M. A. El-Wahed, S. Mesbah, and A. Shoukry, “Efficiency and security of some image encryption algorithms,” in *Proc. World Congress on Engineering*, London, 2008, vol. 1, pp. 2–4.

Mr. V. M. Manikandan was born in Kerala, India, in 1985. He received the Bachelor of Engineering degree in Computer Engineering from Institute of Engineers (India) in 2008, and the M.Tech degree in Software Engineering from Cochin University of Science and Technology, Kerala India, in 2010. He joined at Indian Institute of Information Technology Design and Manufacturing (IIITDM) Kancheepuram, India as a research scholar on January 2014. His current research is concentrated on reversible data hiding and digital image forensics.

Dr. V. Masilamani is an Assistant Professor in the Department of Computer Engineering, Indian Institute of Information Technology Design and Manufacturing, Kancheepuram, Chennai, India. He has received his Ph.D., in Computer Science and Engineering from Indian Institute of Technology Madras, India. Previously he received his M.Tech in Computer Science from Indian Institute of Technology Kharagpur, India. He is working in theoretical and application aspects of image processing.