International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 15 (2018) pp. 12373-12378
© Research India Publications. http://www.ripublication.com

Data Security Using Nested Randomization and Lossless Compression Techniques

[1]Ms. LavanyaKandikunta, [2]Mrs. B. Hari Chandana, [3]Prof. T. Bhaskar Reddy

*[1, 2, 3]Department of Computer Science and Technology, Sri Krishnadevaraya University,
Anantapur-515003, Andhra Pradesh, India.*

Abstract

Data Security plays a major role in the digital era. However, the data stored in internet clouds of various industrial servers, still we have the issues of data theft and fraudulent activities. Which brings out the innovation of adaptive and novel techniques for better data security in securing and providing very high privacy to the data stored in unanimous servers. This paper proposes a novel approach, which enables to generate a crypt image incorporating multiple gray images in special domain. It involves steganography of eight 8-bit images into a single 32-bit crypt image For this process we are undergoing segmentation of the resulted merged image. That segmented image is shuffled using Nested Image Randomization Technique. Here we have used Lossless Predictive coding compression technique for better compression and retrieval of image without loss. After steganography, shuffle and compression operations are applied on eight images, we obtain an image, which has become very hard to be identified. This shows that our approach can protect the privacy of images, which makes image could be stored to public cloud. In addition, people may still be able to see the compressed image even though they have never extract the original images. Data security is applied for improving the security.

Keywords: Data security, Cryptography, Nested Randomization, Image Segmentation, 8-bit, 32-bit images, Lossless Compression, Steganography.

INTRODUCTION

For decades, people have endeavored to develop pioneering techniques for secret communication. In fact, Cryptography and Steganography are two popular techniques intended to protect and safely transmit secret data. The former scrambles information so that it becomes unreadable by unauthorized parties; whereas, the latter conceals the very existence of information by embedding it into a carrier medium such as image, audio file, video file, or text file [1]. In this respect, steganography can be considered as a stealthy method for secret communication as it hides the existence of communication, so much so that no one apart from the sender and the receiver would suspect any piece of data being communicated.

Fundamentally, steganography is an information hiding technology that covers data into digital media files. Its applications are diverse, including secret communication, copyright protection, digital watermarking, and tamper proofing [2]. In practice, steganography works as follows: A message that needs to be secretly communicated is first encoded into a digital carrier file such as an image file. Then, the carrier is transmitted to the intended recipient, who upon reception, decodes it and eventually recovers the covered secret message. Obviously, the biggest advantage of steganography is that it hides the fact that a secret communication is taking place; thus, avoiding the detection of the secret message by eavesdroppers and malicious parties [3].

The strength of steganography resides in how strong the carrier medium is imperceptible and how much the covered message is difficult to be detected and uncovered by unauthorized observers. In critical situations, people known as steganalysts are hired to identify suspicious files and detect whether or not they contain secret information, and if possible, recover this information. Actually, developing a steganography algorithm that firmly conceals data in a hard-to-notice, hard-to-detect, and hard-to-recover way ensures that the secret information being communicated through certain carrier medium would pass undetected by forensics and illicit third parties.

This paper proposes a novel steganography scheme for hiding digital data into uncompressed image files using a randomized algorithm. The proposed scheme uses two mediums to deliver the secret data. The first medium is a carrier image holding the secret data inside the LSBs of its pixels which, unlike traditional LSB techniques, these pixels are selected randomly and not in sequence. The second medium is a well-structured and syntactically correct English text made up of several English sentences pointing to the location of the random carrier pixels, that is, the location of the secret data in the carrier image. In effect, the second medium is not predefined but dynamically generated during the encoding process using a mini-version context-free grammar of the English language coupled with a lexicon of English words randomly categorized in 10 categories representing the 10 digits of the decimal system. These digits are used to generate all possible location values for the carrier pixels. The proposed scheme has such advantages as being hard-to-notice, hard-to-detect, hard-to-recover, binary-based, multilingual, and mutable. All in all, they enable it to be used for versatile types of data, in total secrecy, and without getting detected or recovered, tricking stego-analysts and misleading them from the true location of the covert data.

As more and more individuals and organizations stored their data in cloud, there are also concerns about cloud computing, which have affected the wide adoption of cloud [2]. On top of the list are security and privacy concerns. For example, people concern about the storage and processing of sensitive data in remote physical infrastructure that are owned by a third party, i.e., a cloud service provider (CSP). Since a CSP has full control of the data, it is possible that the CSP conduct malicious attacks on users' data for financial or other reasons.

For example, a CSP could make money by revealing the data of one client (say C) to C's competitor. Meanwhile, a client's data may be leaked to the public if a CSP does not have good security mechanisms to protect its servers.

Most existing solutions (e.g., [3], [4], [5]) employ encryption/ decryption techniques combined with access control and auditing to provide security and privacy for data stored on public cloud. However, in doing so, these solutions inevitably introduce a heavy computational overhead on the data owner for key distribution, data management, data query, and other operations.

In this paper, we consider a different approach: achieving data privacy by utilizing hybrid cloud. A hybrid cloud consists of public cloud (such as Amazon EC2) and private cloud, which is owned and controlled by the data owner. The privacy of data is protected by splitting user data into sensitive data and non-sensitive data, and only outsourcing the non-sensitive data to the public cloud. The sensitive data is stored in user's private cloud.

Many data (such as medical data) stored in cloud have a large number of images, which require a lot of storage and computations. A patient medical image may be private. If we directly take advantage of the approach mentioned above, all the medical images need to be stored in private cloud. This would require a large amount of storage in private cloud, and may cause most data stored (and processed) in private cloud, instead of in public cloud. Typically, one wants to minimize the storage and computation in private cloud. To address the above challenge, an important problem: How to efficiently achieve image data privacy by using hybrid cloud? Compared to using public cloud only, using hybrid cloud would have communication overhead between private and public cloud.

Besides achieving data privacy, we want to reduce storage and computation in private cloud, as well as communication overhead between private and public cloud.

Compression and decompression of the data plays a vital role in data storage and management in cloud. The data that has been stored in the cloud has to be secured and should be robust. There are various compression techniques with lossy and lossless of data. In most of the industrial practices where quality and resolution place a major criteria there we use lossless compression techniques so that while decompression of the compressed data any loss of data might reduce the quality of the image and resolution. Here in this project we have implemented a novel Lossless compression Technique with a better compression ration compared to entropy coding algorithms.

In this paper, we propose a novel algorithm that efficiently achieves data privacy for large data sets, especially images, stored in cloud. In our algorithm, firstly, a random noise is added to image blocks instead of pixels, and a balance between the complexity of recovering the image and communication overhead determines the size of block. Then a random shuffle operation is applied on the modified blocks, which makes the image hard to be recognized. To prevent the data from being analyzed, we remove relationship among tables stored in public cloud, using hash functions with different keys.

A. *Bit shifting*

Bit shifting is the technique to get the advantage of middle frequency value. If we change the value of pixel up to middle bit value, image will not disturb a lot. Consider the 8 bit value of an image, convert each pixel value into binary format, each pixel is representing in 8 bit number. The MSB bit is having highest value 128, LSB is having the least value 1 and middle bit value is 16.

B. *Block Wise Segmentation*

We present a new segmentation and modeling scheme for images based on vector quantization, which yields very fast responses and can avoid local minima in the computation. The feature vectors are defined by the local histogram on a block partioned image, and the local histograms are approximated by normal distributions. This is a suitable feature extraction for medical images since most are tone images with short-term correlation. Within this framework, the least relative entropy is chosen as the meaningful distance measure between the feature vectors and the templates. The segmentation is then performed by a block-wise classification-expectation algorithm, and is improved by a multiresolution procedure. The performance of this learning technique is tested with both simulated and real medical images, and is shown to be a highly efficient segmentation scheme.

This method is a combination of three characteristics of the image: partition of the image based on histogram analysis is checked by high compactness of the clusters (objects), and high gradients of their borders. For that purpose two spaces has to be introduced: one space is the one-dimensional histogram of brightness $H = H(B)$, the second space – the dual 3-dimensional space of the original image itself $B = B(x, y)$. The first space allows to measure how compact is distributed the brightness of the image by calculating minimal clustering kmin. Threshold brightness T corresponding to kmin defines the binary (black-and-white) image – bitmap

$$b = \varphi(x, y),$$

Where $\varphi(x, y) = 0$,

$$\text{if } B(x, y) < T, \text{ and } \varphi(x, y) = 1,$$

$$\text{if } B(x, y) \geq T.$$

The bitmap b is an object in dual space. On that bitmap a measure has to be defined reflecting how compact distributed black (or white) pixels are. So, the goal is to find objects with good borders. For all T the measure

$$MDC = G/(k \times L)$$

has to be calculated (where k is difference in brightness between the object and the background, L is length of all borders, and G is mean gradient on the borders). Maximum of MDC defines the segmentation.

RELATED WORK

Wide variety of applications has been increasing in Digital Image Processing. In that there is a large need of internet applications which requires information to be transmitted in a more secured manner. Steganography and Cryptography are widely used techniques for secured transmission of information. Steganography hides the information in cover images. Cryptography convert the plain text into cipher text, this cipher text will be in unreadable format. These techniques are combined together to achieve higher secured transfer of information over communication channel. So, this minimizes threat of intrusion. Compression techniques can be applied to reduce the size of secret-embedded information in order to reduce burden along with secure transmission.

A. ***Multilevel Crypting Approach for Ensuring Secured Transmission of Clandestine Images: KonakantiBhargavi [1].*** Proposes a novel approach, which enables to generate a crypt image incorporating multiple gray images in special domain. It involves merging of two 8-bit images into a single 8-bit crypt image and applying the same technique for two merged 8-bit images, which in turn generates a single 8-bit crypt image. The generated image is subjected to masking and compression. This approach ensures optimum resource utilization (data redundancy, bandwidth, traffic load) along with secure transmission.

B. ***Multilevel Data Encryption Using Hadamard Transform Based Image Steganography: Shweta Dahiya. [2].*** Proposes a concept to design an effective and more secure image steganography algorithm using cryptographic algorithm named multi-level encryption. It is an improved report of existing single level encryption algorithm. In this investigation, the focus of concern is image because it is widely used in internet and also in mobile system. Enhanced Linear Significant Bit (LSB) algorithm can easily be executed and do not corrupt the image to the point of being noticeable. It would appear that improved LSB using Hadamard multi-level transform is more suitable algorithm of steganography due to its security. Using improved LSB algorithm we can exchange secret messages over public channel in a safe way. The proposed method is more secure than previous method which uses only simple encryption because it is totally relied on the number of 1’s in the equivalent binary value of the key.

C. ***An Image Steganography Scheme using Randomized Algorithm and Context-Free Grammar: Youssef Bassil [3].*** Proposes A better approach would be to hide the very existence of the message using steganography. Fundamentally, steganography conceals secret data into innocent-looking mediums called carriers which can then travel from the sender to the receiver safe and unnoticed. This paper proposes a novel steganography scheme for hiding digital data into uncompressed image files using a randomized algorithm and a context-free grammar. Besides, the proposed scheme uses two mediums to deliver the secret data: a carrier image into which the secret data are hidden into random pixels, and a well-structured English text that encodes the location of the random carrier pixels. The English text is generated at runtime using a context-free grammar coupled with a lexicon of English words. The proposed scheme is stealthy, and hard to be noticed, detected, and recovered. Experiments conducted showed how the covering and the uncovering processes of the proposed scheme work. As future work, a semantic analyzer is to be developed so as to make the English text medium semantically correct, and consequently safer to be transmitted without drawing any attention.

D. ***Efficiently Secure Data Privacy on Hybrid Cloud: Xueli Huang and Xiaojiang Du. [4].*** Proposes a novel scheme to achieve the above goals. We test our scheme in real network environments (including Amazon EC2). We also propose a novel algorithm to process private image data. Our experimental results show that: (1) Our algorithm achieves data privacy but only takes about 1/1,000 the time of the AES algorithm. (2) The delay of our hybrid cloud approach (including the private and public cloud communications) is only 3% - 5% more compared to the traditional public-cloud-only approach.

DESIGN AND METHODOLOGY

A. Proposed Technique

Data Privacy and security has been a major concern in the digital era. Providing security to the user data by means of encryption is one of the methods we use in the present digital world. Data theft is the major concern in the field of digital data encryption. Skilled Computer Engineers so called intruders and Hackers of digital world are good at data theft if the data like images encrypted in a single layer of protection. Hence, we have very big concerns for a better security and privacy we are going to use multi-layer protection by adaptive techniques like Nested Randomization Technique.

Design flow of proposed Work:

1. Consider Eight 8-bit images (same sizes).
2. Convert images into pixels and again pixels to

   Binary values.
3. Pick the first pixel from the eight images, andcombine them to get the new 32-bit pixel.
4. Again, take the second pixels from eachimage, consider the first four bits from 8 images and combine them to into new 32-bit pixel.
5. Repeat the above procedure till it reaches lastpixel of both the images.
6. Finally, we get the single 32-bit image, which is an incoherent image.
7. In addition, that incoherent image is segmented into NxN blocks.

8. That segmented image is again shuffled using Nested randomization technique and compression technique is applied to the resulted randomized image.

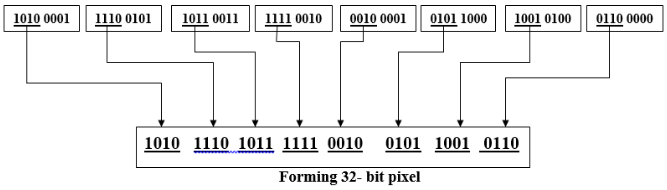


Figure 1: a) Forming 32-bit pixel

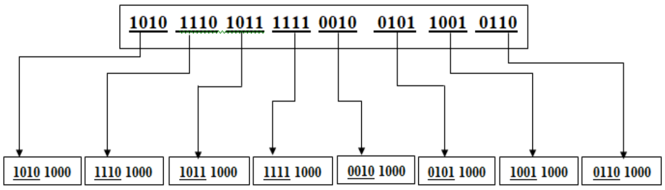


Figure 1: b) Forming 32-bit to eight 8-bti pixels

When reconstructing the image we are replacing LSB 0000 to 1000 by this loss of image that eye cannot be detected.

1111=15 Maximum value.

We are taking the average value is 15/2=7.5~ 8

The binary value of 8= 1000

1010=10 binary value

Here LSB value is 10 but we are replacing with 8 so that image loss is 2. Therefore, the image losswhen compared to maximum value is less.

B. *Proposed Architecture*

The Proposed Architecture consist of cryptography of Digital image with encryption and decryption of the image as shown below:

Step1:

The eight images converted into pixels and again these pixels converted into binary values as explained in the proposed technique step by step. Next, we have done fusion to get the fusion image. In addition, this fusion image undergoes nested randomization.

Step2:

The nested randomized image again converted back to Steganography image and then to respective images using the adaptive techniques and algorithms used.

Step3:

Compression technique is implemented and used for better security by compressing the randomized image and decompressing the compressed image at the receiver end is shown in the images below.

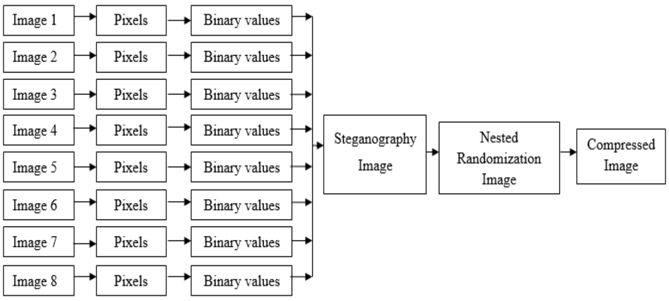


Figure 2: Encrypted Nested Randomized image to compressed image

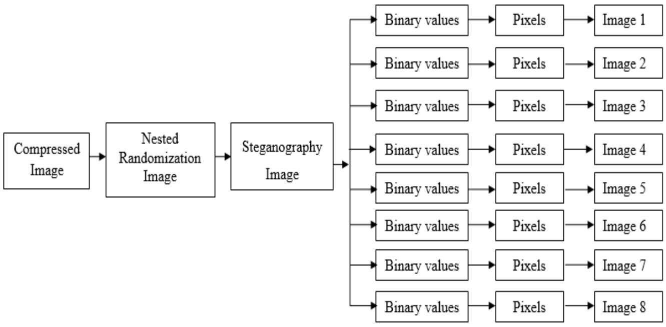


Figure 3: Decrypting Compressed image to Nested Randomized image and to normal images

Proposed Nested Randomization Algorithm:

```
1. row = n;
2. col = n;
3. read the input file
4. get total width and total height of an image
        tWidth = originalImgage.getWidth();
        tHeight = originalImgage.getHeight();
5. get width and height of each segmentation
        eWidth = tWidth / col;
        eHeight = tHeight / row;
6. fetching image files
        for (inti = 0; i< row; i++)
                y = 0;
        for (int j = 0; j < col; j++)
segmentedImgage = Subimage(y, x, eWidth, eHeight);
        outputfile[len] = "img"+k+".jpg";
        y += eWidth;
7.  Nested randam function calling
buffImages[len]=SubRandom(SubImgage,k);
len++;
k++;
                x += eHeight;
8. getting final image
                num = len-1;
        for (inti = 0; i< row; i++)
        for (int j = 0; j < col; j++)
finalImg=Image(buffImages[num], chunkWidth * j,
chunkHeight * i, null);
num--;
9. end of the algorithm
```

C. Compression Technique

In lossless predictive image compression approach [2], inter-pixel redundancies are removed by predicting the current pixel value using closely spaced pixel values and generating new values for coding. The new values represent the error generated from the subtraction of the predicted value from the original value. Figure 4 shows the complete structure of lossless predictive coding system.

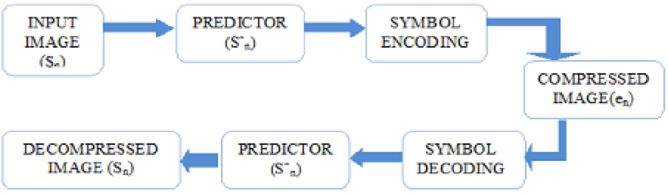


Figure 4. The complete structure of the lossless predictive coding system.

As shown in Figure 4, lossless predictive coding system consists of two parts, the transmitter and the receiver. At the transmitter, the current pixel value is predicted using the closely spaced neighborhood pixel values. The predicted value is generated using linear weighted combination of the previous pixel values as follows [2]:

$$X(r, c) = X(r, c - 1) - X(r - 1, c - 1) + X(r - 1, c)$$

To predict the pixels of an image block, we will use the predictor equation as shown above

$$\hat{S}_n = \text{round}\left[\sum_{i=1}^{m} w_i S_{n-i}\right]$$

Wherewi are the predictor parameters and the linear combination of the previous pixel values is rounded to its nearest integer value. The difference between the original and the predicted signal values:

$$e_n = S_n - \hat{S}_n$$

will be transmitted to the symbol encoder in which a variable length coding system is provided to encode the error value. It may argue that this is a lossy rather than lossless image compression method because of the rounding operation at the transmitter. However, since there is no quantiser, the technique is considered lossless.

At the receiver, the same predictor is provided. The coded error signal is added to the predicted signal $\hat{S}_i$ to produce the original signal:

$$S_n = e_n + \hat{S}_n$$

The compression of the image is performed using variable length coding where coding redundancy is removed and the prediction operation provides the elimination of the inter-pixel redundancy.

RESULTS AND DISCUSSION

The implementation of the proposed work done using the following dataset, which contains eight different images of same size.

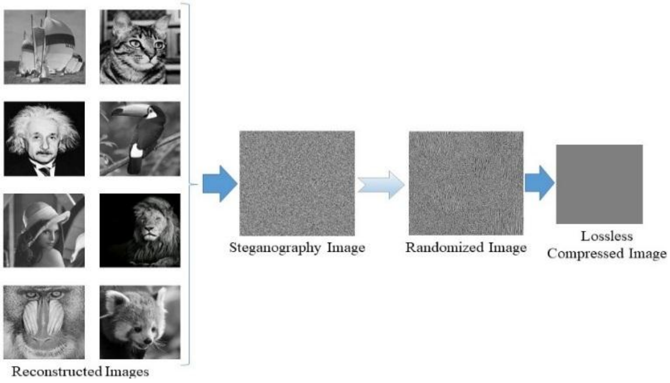


Figure 5: Results of Steganography Image with Eight Images

As Shown in the Figure 5, we have used the dataset of 8 images with same size. After Fusion of 8 images using the Steganography technique explained in the proposed work. We achieved a Fusion image that has been further proceeded for Nested Randomization Process.

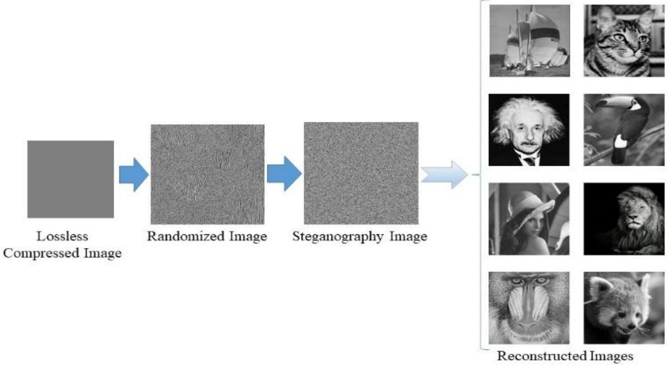


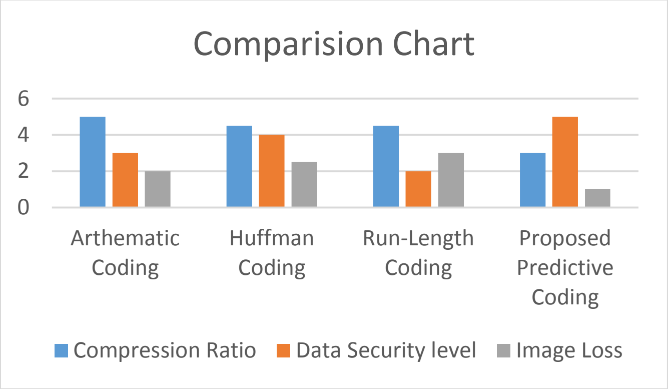
Figure 6: Results of Randomized Image

As shown in the Figure 6, we can see the fusion image is further processed for Nested Randomization and we have got the Randomized Image.

We have done 20*20 Block segmentation and randomization using Nested randomization Technique.

The randomized image is compressed using Lossless predictive Coding technique. Which gives the advantage of removing Inter-pixel Redundancy.

Compression Technique	Compression Ratio	Data Security Level
Athematic Coding	Low	Medium
Huffman Coding	Low	Better
Run-Length Coding	Low	Low
Lossless Predictive Coding	Better	High



From the analysis and implementation of lossless predictive compression technique, we were able to provide high security with low compression ratio.

CONCLUSION

The Motive and purpose of the thesis is to provide better and more efficient way of Securing Digital data from falling prey to the fraudulent and hackers. By using Multi-level Steganography and Randomization Techniques, we have successfully analyzed and experimented using the Eigth 8-bit image dataset. The incoherent image obtained after successful Randomization undergoes lossless predictive image compression, which is far secure and efficiently compressed which cannot be decrypted or decompressed. The obtained results prove that Lossless compression techniques use less compression ration and provide better data security by the integration of our proposed nested randomization techniques.

FUTURE SCOPE

- As we can see the compressed image has to be properly masked then compressed and encrypted using advanced Image encryption standards and integrated to the cloud.
- Encryption and cloud computing for Data security for digital data can be obtained with further study and implementation.
- We can implement this technique in color images also.

REFERENCES

[1] Multilevel Crypting Approach for Ensuring Secured Transmission of Clandestine Images by Konakanti Bhargavi, Thota Sri Harish Reddy, Thota Bhaskara Reddyat 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT).

[2] Image Compression Techniques: A Survey in Lossless and Lossy algorithms. A.J. Hussain , Ali Al-Fayadh , NaeemRadi PII: S0925-2312(18)30293-5, DOI: 10.1016/j.neucom.2018.02.094.

[3] Multilevel Data Encryption Using Hadamard Transform Based Image Steganography: Shweta Dahiya. 2016 IJEDR | Volume 4, Issue 4 | ISSN: 2321-9939.

[4] An Image Steganography Scheme using Randomized Algorithm and Context-Free Grammar: Youssef Bassil. Journal of Advanced Computer Science and Technology (JACST), ISSN: 2227-4332, Vol. 1, No. 4, December 2012http://www.sciencepubco.com/index.php/JACST/article/view/512/424.

[5] Efficiently Secure Data Privacy on Hybrid Cloud: Xueli Huang and Xiaojiang Du, Published 2013 in 2013 IEEE International Conference on Communications (ICC).

[6] S. Rohith, K. N. H. Bhat and A. N. Sharma, “Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register”, Proc. Of International Conference on Advances in Electronics, Computers and Communications(ICAECC), 2014, DOI: 10.1109/ICAECC.2014.7002404.

[7] S. V. Sathyanarayana, M. A. Kumar and K. N. Hari Bhat, “Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points”, International Journal of Network Security, vol.12, no.2, pp.166–179, 2011.

[8] S. Sowmya and S. V. Sathyanarayana, “Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)”, International Conference on Contemporary Computing and Informatics (IC3I), 2014, DOI: 10.1109/IC3I.2014.7019665

[9] S. Das, S. N. Mandal and N. Ghoshal, “Multiple-Image Encryption Using Genetic Algorithm”, Advances in Intelligent Systems and Computing, vol. 343, pp. 145-153, 2015.

[10] Image compression techniques using Modified high quality multi wavelets AuthorsDr.T.Bhaskara Reddy M.AshokPublication date2011JournalIJACSAVolume2Issue7Pages153-158Publisher2158-107X.

[11] A Novel Approach of Lossless Image Compression using Hashing and Huffman Coding Authors Mrs. T. Anuradha Dr. T. Bhaskara Reddy , Miss. Hema Suresh Yaragunti ,,Dr. S. Kiran Publication date 2013 Journal International Journal of Engineering Research & Technology (IJERT) Volume 2 Issue 3 Publisher ISSN: 2278-0181.

[12] Hidden security features for the recognition of fake currency by B.Harichandana, Lavanya.K, Prof.T. Bhaskara Reddy International Journal of Advanced Research in Computer Science. Mar/Apr2018, Vol.9 Issue 2, p292-299. 8p.

[13] Gonzalez, R. C and R. E. Woods. (1992). Digital image processing, Addison-Wesley, Reading, pp. 307-411.