A Generic Reversible Water Marking and Encryption Scheme Based on Histogram Processing

Aparna Krishna[1], Bijin Bodheswaran[2]
[1]*M .Tech student, Sree Buddha College of Engineering, Elavumthitta, Kerala, India*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering, Elavumthitta, Kerala, India*

***Abstract*- Reversible data hiding (RDH) is an active area of research in signal processing. In this paper a reversible data hiding (RDH) algorithm is proposed for digital images. The traditional RDH algorithms have a disadvantage that it is not robust in nature. Here in this paper the focus is laid on increasing the robustness of the RDH algorithm, this is achieved through scrambling and encryption. The scrambling of the input image is done by using Arnold transform and encryption is done based on XOR operation. By changing the position of the watermark image pixels through Arnold transformation the better secret watermark information can be hidden with the host image and the overall security can be improved by the technique of encryption. Here the algorithm not only keeps the PSNR value high but also increases the contrast of the image thereby increasing the visual quality of the image. It is the first RDH algorithm that incorporates both scrambling and encryption to increase the security of the algorithm .The proposed system produced better results compared to other existing RDH algorithms so this methods can be used in real time multimedia based secure communication systems.**

***Index Terms*- RDH, Arnold scrambling, Encryption, visual quality, histograms.**

I. INTRODUCTION

DATA HIDING is commonly referred to as a process where details are hided into a cover media. That is, by the data hiding process two sets of data's are linked, a set of the embedded data and another set of the cover media data. In covert communications, hidden data may often be considered irrelevant comparing to the cover media. In authentication, the embedded data and the cover media are closely related. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, due to the data embedding process the cover media will experience some distortion and it cannot be inverted back to the original media. That is, even after the extraction process some permanent distortion will still occurred to the cover media. In some applications, such as medical diagnosis and law enforcement due to some legal considerations it is very important to reverse the watermarked media back to the original cover media after the data extraction that is no change of the cover medium is allowed. In other applications which are highly sensitive, such as remote sensing and high-energy particle physical experimental investigation, it is desired that the original cover media can be recovered because of the required high-precision nature. The techniques satisfying this requirement of lossless data recovery along with the reversible cover medium are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques.

Reversible Data Hiding (RDH) [3] is a field that has been popularly studied in the community of signal processing. The main purpose of RDH algorithm is data hiding that is to embed secret information into a host signal such that a marked one is generated, from this marked one the original signal can be recovered exactly after extracting the embedded data from it. The main tools to evaluate the RDH algorithm performance are the hiding rate of RDH and the marked image quality [5]. There usually exists a trade-off between these two because increasing the hiding rate often causes more distortion in the content of the host image thereby decreasing the visual quality. Direct modification of histogram of the image provides less embedding capacity [7]. Comparing with other data hiding techniques that is commonly used, the specific property of RDH is that it can perfectly recover the cover medium and the

secret data that is embedded. In general, RDH is a fragile technique and it poses no robustness against possible attacks.

The traditional RDH algorithms have a disadvantage that it is not robust in nature [1]. Here in this paper the focus is laid on increasing the robustness of the RDH algorithm. Many methods are existed in RDH that incorporates encryption with RDH jointly referred to as RDH-EI. This is achieved through scrambling [11] and encryption [8]. The scrambling of the watermark image is done by using Arnold transform [12] and encryption is done by using X-OR operation [8]. By changing the position of the watermark image pixels through Arnold transformation, the better secrecy watermark information can be hidden with the host image. Thus there is a doubly secured RDH algorithm developed. Considering the images that are obtained with poor illumination, in such cases improving the visual quality is more important than keeping the just keeping the PSNR value high. Moreover, in medical or satellite images for visual inspection purposes the contrast is needed to be considered as a primary issue so contrast enhancement of such images is very important.. The RDH algorithm that is proposed here can also use to achieve the property of contrast enhancement instead of just keeping the PSNR value high [1]. Generally, image contrast enhancement can be achieved by histogram equalization. To perform the processes of data embedding and contrast enhancement at the same time, the proposed algorithm modifies the histogram [7] of pixel values. Firstly, the two peaks in the histogram are selected then these bins are used to modify each of the pixels in the image thus by this modification process the histogram will become more and more equalized than the original histogram of the image to avoid the overflows and underflows that occur due to histogram modification, the bounding pixel values are pre-processed and a location map is generated to memorize their locations of the preprocessed pixels. The visual quality can be preserved after a considerable amount of message bits have been embedded into the host the proposed system produced better results compared to other existing reversible data hiding algorithms [1] so that we can use this method in real time multimedia based secure communication systems

The section 2 presents the details of the proposed RDH algorithm Section 3 presents the procedure for the RDH algorithm, Section 4 gives details about simulation results and the advantages of the proposed algorithm are given in section 4. Finally, a conclusion is drawn.

II. ROBUST RDH ALGORITHM WITH CONTRAST ENHANCEMENT

A. Data Embedding

Consider an 8-bit gray-level image, let the image be I, the image histogram can be plotted by counting all the pixels with intensity value j for j∈{0,1,…254,255}. Here h_I is denotes the image histogram of the image so that h_I(j) represents the number of pixels with a particular intensity value j.. N non empty bins are present inh_I, from which the two peaks i.e. the highest two bin are chosen. The highest two bins corresponding smaller and bigger values are denoted byI_S andI_R , respectively. Data embedding is performed for a pixel counted in h_I by,

$$i' = \begin{cases} i - 1, & \text{for } i < I_S \\ I_S - b_K, & \text{for } i = I_s \\ i, & \text{for } I_s < i < I_r \\ I_S + b_K, & \text{for } i = I_R \\ I_S + 1, & \text{for } i > I_R \end{cases} \quad (1)$$

i’ is the modified pixel value, and b_k is the k-th message bit (0 or 1) that is needed to be hidden. By applying Eq. (1) to every pixel counted in⟦ h⟧_I, a total of h_I(I_s) + h_I(I_R) binary values are embedded in it. Last split peak value is needed to be known during the extraction process. One way is to is to exclude 16 pixels in image from histogram computing that is the value of the last split peaks are embedded at the LSBs of these excluded pixels.. The least significant bits (LSB) of excluded pixels are collected and included in the binary values to be hidden. After applying Eq. (1) to each pixel counted in h_I for data embedding, the values of I_S and I_R (each with 8 bits) are used to replace the LSBs of the 16 excluded pixels by bitwise operation. To extract the embedded data, the peak values need to be retrieved and the histogram of the marked image I^' is calculated excluding the 16 pixels aforementioned. Then the following operation is performed on any

pixel counted in the histogram and with the value ofI_S-1,$I_S$$I_Rori_R$ +1

$$b_{k'} = \begin{cases} 1, & \text{for } i' = I_S - 1 \\ 0, & \text{for } i' = I_s \\ 0, & \text{for } i' = I_R \\ 1, & \text{for } i' = I_R + 1 \end{cases} \quad (2)$$

Where K-th binary value extracted from the marked image I^'is〖 b〗_K^'. According to Eq. (1), the embedding process take place and according to Eq. (2) the extraction takes place. Now for the recovery operation the following operation is performed on every pixel counted in the histogram to recover its original value:

$$i = \begin{cases} i' + 1', & \text{for } i' < I_S - 1 \\ I_S, & \text{for } i' = I_s - 1 or\ i' = I_s \\ I_R, & \text{for } i' = I_R\ or i' = I_R + 1 \\ i' - 1', & \text{for } i' > I_R + 1 \end{cases} \quad (3)$$

The original LSBs of 16 excluded pixels are obtained from the extracted binary values. The excluded pixels can be restored by writing them back so as to recover the original image.

B. Preprocess

In this algorithm, it is required that all pixels counted in the histogram of the image h_I are within{1,2,…254} . If there is any bounding pixel values present either 0 or 255, then it may cause overflow or underflow. To avoid the overflow or the underflow the histogram needs to be pre-processed before the histogram modification operations. Specifically, all the pixels having values 0 and 255 are changed to 1 and 254, respectively. Since it is an RDH algorithm no permanent change of the host image is permitted so all the preprocessed pixels also needed to be written back, for this purpose a location map is make use hereto memorize the pre-processed pixels, a location map whose size is same as that of the image is used. A location map with the same size as the original image is generated by assigning 1 to the location of a modified pixel, and 0 to that of an unchanged one (including the 16 excluded pixels). By restoring the original values of those pixels accordingly, the original image can be completely recovered.

C. Scrambling

In data hiding one of the important metric used for the quality analysis is its security or its robustness. Generally the RDH algorithms are not truly secured, one of the methods to increase the robustness of the RDH algorithm is by adding scrambling in to the system. Here the data that is needed to be hided is scrambled such that the confidentiality of the content is well preserved that is by making image visually unreadable the security of the image can be preserved and also it will be difficult to decrypt it for unauthorized users this method is referred to as image scrambling. During a particular class of transformation, digital image scrambling usually make an image into a completely different meaningless image and it is like a pre-processing during information hiding of the digital image, which also known as information disguise. Image scrambling technology is a data hiding technology which is a non-password security algorithm for information hiding. There are various image scrambling techniques currently in the area of image processing that that can be used to encrypt images efficiently by scrambling the images.Arnold scrambling algorithm is one among them which is widely used. Due to its feature of simplicity and periodicity it is used widely in the digital watermarking technology. the original image can be restored after several cycles due to the periodicity of Arnold scrambling that is it has to wait for a long time to restore an image because the periodicity of Arnold scrambling depends on the image size, if the size of the image is too high then restoring process will be too long Generally, the image degree and the cycle of Arnold transformation is not directly proportional. The algorithm for the Arnold scrambling is as follows;

The transformation of point (x, y) to another point (X ', Y ') in the unit square change by Arnold scrambling algorithm is defined by the equation;

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod } (1) \quad (4)$$

We need to change the two-dimensional Arnold scrambling of mod 1 to mod (N) to be specific to the digital image then the equation changes in to:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod } (N) \quad (5)$$

If N is the order of digital image matrix then the value of the x, y will be x, y €{1,2,3,…(N-1)}. The digital image can be seen as a two-dimensional matrix. When the size of the image is N, then the image have N × N elements, here the subscript x, y stand for the position of pixel, x, y ∈ {0, 1, 2..., N-1}. Let x, y that is defined previously corresponds to the x, y of Arnold scrambling. Then for each pair x, y, after Arnold scrambling will become X' and Y'.This can be defined as the original image of the point from (x, y) move to the point (X ', Y') so that way the movement of pixels in the image take place. In the image where Arnold scrambling took place then it will traverse all the points to complete a new picture, a scrambled picture. The cycle of Arnold scrambling and the size of the image are related.the corresponding two dimensional Inverse Arnold transformation matrixes is as follows:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod (N) \qquad (6)$$

D. Image Encryption

The process involve here is the technique of the simple XOR operation for the image encryption For example, the string (01010111 01101001 01101011 01101001) can be encrypted with the repeating key 11110011.Then the encrypted string is (10100100 10011010 1011000 10011010),conversely for decryption the output string is (01010111 01101001 01101011 01101001) this is again obtained by the XOR operation between the encrypted string and the key 11110011 .The encryption used here is a private key or symmetric key encryption process, that is the key used here is same for both the encryption and the decryption process. The key that we used here is the binary value of 256.The key should be transfer between the transmitter and the receiver prior to the whole data transfer process.

III.PROCEDURE FOR THE RDH ALGORITHM

Reverse data hiding is a technique is used to hide a secret data in to a host image preventing the object's data details. This technique is used to ensure the security and to protect the integrity of the object from any modification by preventing intended and unintended changes.

A. Embedding Section

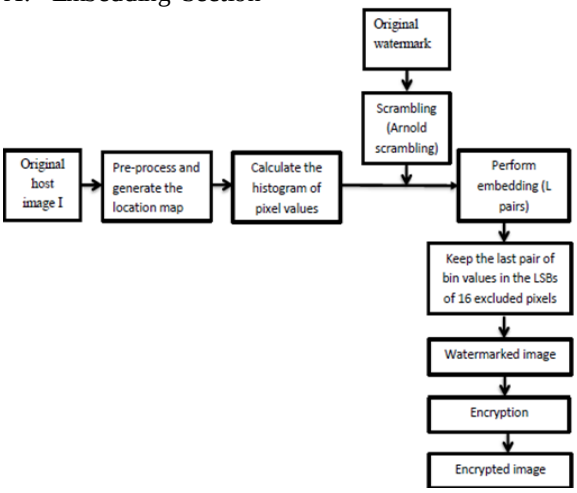

Fig: 1 Embedding processing

The procedure for the embedding section of the proposed RDH algorithm is shown in Fig 3. 1. totally L pairs of histogram bins are to be split for data embedding and the value of L is determined by the transmitter based on the amount of data to be hided and the amount of contrast enhancement the person needs, the embedding procedure includes the following steps:

1. Pre-process: in the pre-processing the pixels in the range of [0, L-1] and [256-L, 255] are processed as mentioned in section 2.2 but it is done by excluding the first 16 pixels in the bottom row. To record the locations of those pixels a location map is generated and it is compressed to reduce its length by the JBIG2 standard.
2. Without counting the first 16 pixels in the bottom row the image histogram is calculated.
3. Arnold scrambling is done on the watermarked image that is the image that is needed to be hided
4. Embedding: the highest two bins in the histogram are split for data embedding by applying Eq. (1) to every pixel counted in the histogram. Then to further increase the embedding rate the two peaks in the modified histogram are again chosen to be split, and so on the process continues until defined L pairs are split. For the perfect recovery operation the bit stream of the compressed location map is embedded before the message bits. LSBs of the 16 excluded pixels are replaced by the last split peak values to form the marked image.

5. By using encryption based on XOR operation an encrypted image is produced. Here we are using a private key encryption process so the key used for encryption is needed to be shared between the transmitter and the receiver prior for the decryption process in the absence of the key the receiver can't do the decryption. The key will be also in the binary format

B. Extraction and Recovery Section

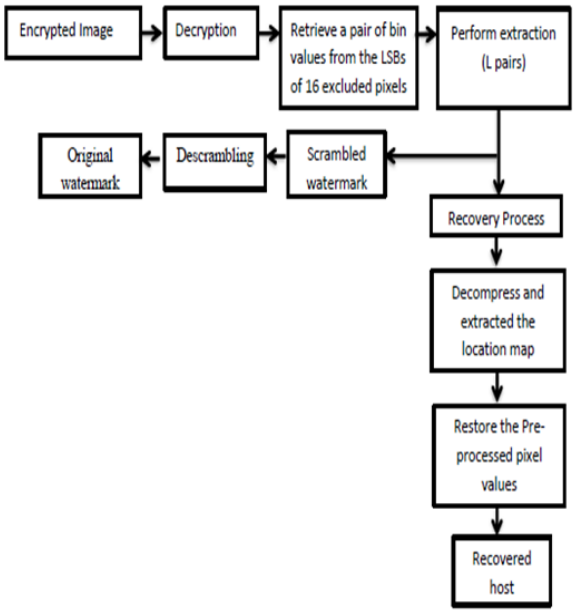

Fig.2. Extraction and Recovery Process

The extraction and recovery process include the following steps:

1. Decryption is done on the encrypted image from the transmitter section. It is done by using the predefined key shared between the transmitter and receiver.
2. for obtaining the last two split peaks the LSBs of the excluded 16 pixels are retrieved
3. By using Eq. (2) the data embedded with the last two split peaks are extracted from this the value of the original LSBs of 16 excluded pixels, the length of the compressed location map, and the previously split peak values are obtained.
4. From the step 2 scrambled watermark is also obtained ,descrambling is done on the scrambled watermark and original watermark image is obtained
5. The recovery operations are carried out on rest of the image from step 2 by processing all pixels except the 16 excluded ones with Eq. (3).
6. The process of extraction and recovery is repeated until all of the split peaks are restored.
7. The compressed location map is obtained and decompressed to the original size that is the size of the image. All those pixels modified in preprocess are identified with the help of the decompressed map. At last, by writing back the original LSBs of 16 excluded pixels the original image is recovered.

IV.SIMULATION RESULTS

The algorithm that is proposed here preserves the image contents confidentiality, this is done by the scrambling and encryption process another importance or characteristic of this algorithm is that it increases the contrast of the host image. To perform this data embedding and contrast enhancement is done at the same time in other words they are simultaneously performed. It is done by the process of histogram modification thereby achieving histogram equalization that increases the contrast of the host image. To increase the embedding capacity, the highest two bins in the modified histogram can be further chosen to be split, and so on until satisfactory contrast enhancement effect is achieved, further the robustness is achieved by scrambling and encryption. The RDH algorithm defined here consist of two basic sections or stages

1. Data embedding stage(Transmitter section)
2. Data extraction and recovery stage (Receiver section)

A. Transmitter Section

In the transmitter section two processes are taking place other than the scrambling and encryption. They are the preprocessing and data embedding. In the transmitter section, an image is taken and considered as the host image. The image to be hidden is embedded into the host image using the Eq. (1). The figure shown below describes the first stage of the data embedding .It mainly includes the host image in which the data embedding take place, the foremost step is to plot the histogram of the image. Here cameraman is used as the host image with size 512*512.the histogram of cameraman is plotted. Then the pre-process is done it mainly depend on the value of L. we plotted the histogram of the pre-processed image, it is clear from the image that the

histogram of the pre-processed image is entirely different from that of the original image histogram. The pre-processed image histogram is more shifted towards the centre that all the boundary pixels is now changed to prevent the overflow and the underflow conditions that take place during the embedding section.

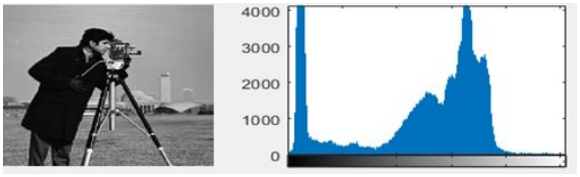

Fig.3 Input image And Histogram

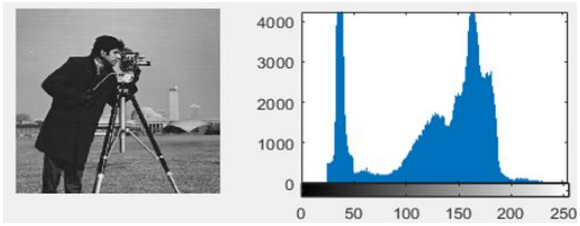

Fig.4 Preprocessed image And Histogram

In the next section scrambling and encryption is done. Here the input image which is needed to be hided is provided, then scrambled version of the input image is produced, the scrambled version of the image is shown in fig 5 (b). Then the watermarked image is produced from the host and scrambled input image shown in fig 5 (c). Later encryption is done to produce an encrypted image as shown in fig 5 (d). The decryption of this encrypted image is needed to be done at the receiver. The scrambling is done by the Arnold scrambling and the encryption is done by XOR operation. Before the encryption the key for encryption the key is needed to be transferred between the transmitter and receiver for decryption. Here we used a private key cryptographic method for the encryption.

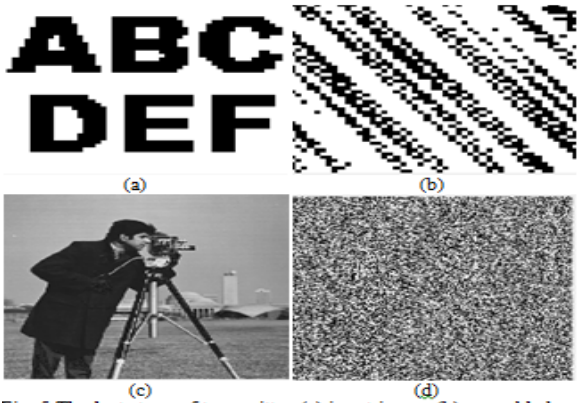

Fig. 5 The last stage of transmitter (a) input image (b) scrambled image (c) watermarked image (d) encrypted image

A. Receiver Section

In the data extraction stage using the defined algorithm the hided image is completely recovered from the watermarked image. The received encrypted watermarked image is used for data extraction. First step is the decryption process, after that the extraction of data which is embedded in host image is done. The extraction process is followed by the scrambling to obtain the embedded data. Then recovery operation takes place by predefined equations. The process of extraction and recovery is repeated until all of the split peaks are restored and the data embedded with them are extracted. The contrast of the host image is also increased.

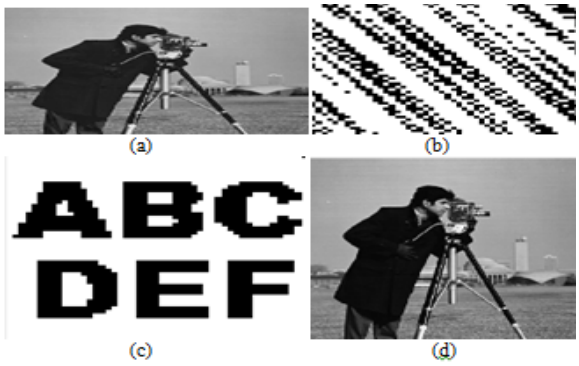

Fig.6 The receiver section (a) decrypted image (b) scrambled image (c) recovered input image (d) recovered host image

C. Contrast Enhancement

In this algorithm the contrast of the host image is increased simultaneously by the data embedding process. This can be proved by plotting the histogram of the host image before and after the process. We can see that once the contrast is increased the histogram will become more equalized than before. here we are taking cameraman image first we plotted the histogram of the host image and then the histogram of the final image after the recovery process is plotted ,by comparing both it is clear than based on the value of L embedding capacity has increased simultaneously the contrast is also increased.

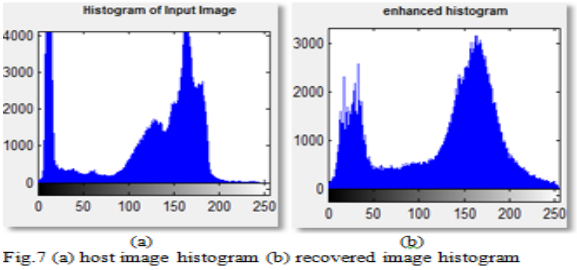

Fig.7 (a) host image histogram (b) recovered image histogram

V. ADVANTAGES

- By splitting of number of histogram peaks pair by pair the contrast of the image can be increased remarkably. By choosing the value of the number of peaks to be spitted we can control the contrast of the image
- This technique can be easily extended to color images.
- Original signal can be exact recovery of the original host data takes place after the extraction of the embedded data.
- It is useful in sensitive applications where no permanent change is allowed on the host signal during the process.
- It protects the image content's confidentiality.

VI. CONCLUSION

A new highly secured reversible data hiding algorithm is developed with the property of contrast enhancement. Here the robustness of the RDH algorithm is ensured through scrambling and encryption. Basically, the two peaks (i.e. the highest two bins) in the histogram are selected for the process of data embedding so that histogram equalization can be simultaneously performed along with the data embedding by repeating the process.The contrast enhancement is achieved by histogram equalisation. The results have shown that the image contrast can be enhanced by splitting a number of histogram peaks pair by pair. Moreover, the original image can be exactly recovered without any additional distortion. Here the robustness of the system is increased .The set of experiments is done on the cameraman image. The contrast enhancement is proved by plotting the histogram of the original image histogram of the recovered image. The proposed system produced better results compared to other existing reversible data hiding algorithms so that we can use this method in real time multimedia based secure communication systems.

ACKNOWLEDGEMENT

I would like to express profound to my guide Mr. Bijin Bodheswaran for his encouragement and for providing all facilities for my work. I would like to extend my gratitude to our Head of the Department Ms. Sangeeta T. R and for providing the necessary guidance and serious advice for my work.

REFERENCES

[1] Hao-Tian Wu, and Jean-Luc Dugelay Reversible Image Data Hiding with Contrast Enhancement IEEE, vol. 20, pp. 569–571, july. 2015.

[2] J. Tian, "Reversible data embedding using a difference expansion, "IEEE Trans.Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar 2

[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for the reversible watermarking, "IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007

[5] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," IEEE Signal Process. Lett. vol. 14, no. 4, pp. 255–258, Apr. 2007.

[6] X. Li, B. Yang, and T. Zeng , "Efficient reversible watermarking based on adaptive an prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Jan. 2011

[7] Z. Zhao, H. Luo, Z.-M. Lu, and J.-S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," Int. J. Electron. Commun. (AEÜ), vol. 65, pp. 814–826, 2011

[8] Piyush Kumar Singh , Ravi Shankar Singh and Kabindra Nath Rai "An Image Encryption Algorithm based on XOR Operation with Approximation Component in Wavelet Transform" IEEE ,Nov,2015

[9] X. Li, W. Zhang, X. Gui, and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 2016–2027, Sep. 2015

[10] Prarthana Madan Modak, Dr. Vijaykumar Pawar "A Comprehensive Survey on Image Scrambling Techniques" International Journal of Science and

Research (IJSR), Volume 4 Issue 12, December 201

[11] Gajendra Singh Chandel and Vinod Sharma "X-OR and Arnold Cipher Based Double Phase Image Encryption Technique" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-4, Issue-12),December 2015

[12] Min Li, Ting Liang and Yu-jibe He "Arnold Transform Based Image Scrambling Method", Atlantis Press, march 2013