Secure Patients Data Hiding Using Integer Transfer

[1]Mr. Ankush R. Patil, [2]Prof. V. K. Patil

Department of E & TC Engineering
D. N. Patel COE, Shahada, India,

***Abstract*— This letter proposes reversible contrast mapping (RCM) watermarking. RCM watermarking involves the transformation of pixel pairs belonging to the RCM domain. RCM is invertible procedure, because even if the least significant bits (LSBs) of the transformed pixels are forfeit. The data space occupied by the LSBs is expedient for biomedical images hiding. The embedded biomedical information bit-rates of reversible watermarking scheme are highest bit-rates till date. The scheme does not require additional data compression, and, in terms of mathematical complexity, it comes into sights to be the lowest complexity one proposed up to now. A very fast lookup table exercise is recommended. Also robustness against cropping can be guaranteed.**

***Keywords:* Steganography, reversible contrast mapping, information hiding, least significant bit, pixel pairs.**

I. INTRODUCTION

Recently data hiding over images have drawn tremendous interest, using either lossy or lossless techniques. Reversible contrast mapping (RCM) is one of the easy integer transform procedure that is applied to the pairs of pixels which can be row wise or column wise. RCM having the high embedding bit rate and the other benefit is it is having low mathematical complexity. Effective adaptation over previously scheduled RCM is suggested here that offers a better trade-off in optical quality-embedding rate-security of the hidden biomedical data. For reversible watermarking the paths proposed so far incorporate a lossless data compression stage. The benefit of a convoluted data compression stage upturn the mathematical complexity of the watermarking. In this paper, we discuss a contrast mapping procedure which is reversible watermarking technique that gain high data embedding bit rate beyond any additional data compression stage. This proposal is based on the reversible contrast mapping (RCM), a walkover integer transform defined on pairs of pixels. RCM is the invertible procedure, because there is no effect on this procedure though least significant bits (LSB) of the pairs of pixel are misplaced. The data space confiscation by the LSBs is reasonable for biomedical data concealing. Here, a mutated translation that admits robustness in opposition to cropping is proposed. Contrast mapping procedure having very low mathematical complexity. Finally, RCM system is correlate with difference expansion system with respect to the bit rate hiding volume and to the mathematical complexity.

II. LITERATURE REVIEW

In general, security means "the quality or state of being secure to be free from any risk" (Whitman, 2007).

The main objective of the project is to propose the method and properties which help to transmit the information over a network without any modifications. The main characteristics of information are

The Availability: The avoidance of unauthorized declaration of information is called the availability. It grant users who need approach the information to do so without any interference and to receive it in the original format. Availability of data needs the authentication of the user as one with authorized access to information (Whitman, 2007). The availability is defined as "Ensuring timely and reliable access to make use of the information or the data. A loss of availability is the confusion of access to or use of data" (Stallings, 2007).

The Accuracy: The information is deemed accurate if it does not contain any mistakes / errors and possesses the value that end user expects. If the data holds a value different from that of the end user's expectations because of known or unknown variations of its data it becomes no longer correct(Whitman, 2007).

The Authenticity: Authenticity shows the quality or state of being original. It should not be a reproduction any previously known data. The Information is called authentic when it is formerly created, placed, stored or transferred. Authenticity is make sure that all the data remains in its original state by stopping any ways of the unauthorized modification of information (Whitman, 2007).

The Confidentiality: "The confidentiality is the state of blocking disclosure or Exposure to unauthorized individuals or system". Confidentiality is the privacy and secrecy which means protection of secret data or that of data belonging to an organization. Confidentiality of content ensures that only those with the rights and privileges access a particular set of data and prevent from unauthorized access (Whitman, 2007).

The Integrity: It is the prevention of unauthenticated modification of data. Integrity of any type of data is inactive when it is subjected to damage (external / internal), destruction or other disruption of its authentic state by intended or unintended sources (Whitman, 2007).

The original/actual bits representing the watermark are scattered throughout the file in such a pattern that they cannot be identified and manipulated. All watermarking methods consists
an embedding system and the watermark extraction or recovery system. Inputs for the embedding systems are cove (data/image),
hiding medium (I), watermark symbol, (w) (image/text/number) and a key (k). Watermarked data/image is the output of embedding system.

A. Reversible Watermarking

Most existing data-embedding algorithms distort the original signal in an irreversible manner and then one of the challenges is to minimize distortion against capacity. But there are various applications, e.g. in medical or military imaging, where any distortion, no matter how small, is intolerable. In such cases one has to take recourse to reversible (also called lossless) data embedding methods. This means that the original signal can be recovered after extraction of the message (or watermark). Such reversible embedding is possible at all, is because of the images usually possess strong spatial correlations.

The watermark substitutes the LSBs of the transformed pairs. At detection, in order to extract the watermark and to restore the original pixels, each transformed pair should be correctly identified. The LSB of the first pixel of each pair is used to indicate if a pair was transformed or not: "1" for transformed pairs and "0" otherwise.

The inverse RCM fails to recover the pairs (a, b) $\in$ D composed of odd values. Such pairs can be used as well for data embedding as long as they are correctly identified at detection. This can be easily solved by setting the LSB of the first pixel to "0." At detection, both LSBs are set to "1" and (2) are checked. If (2) are fulfilled, the pair was composed of odd pixels. In order to avoid decoding ambiguities, some odd pixel pairs should be eliminated, namely, those pairs located on the borders of D. The pairs subject to ambiguity are found by solving in odd numbers the equations: 2a-b=1, 2b-a=1,2a-b=L and 2b-a=L. For L=255 there are only 170 such pairs.

III. BIOMEDICAL DATA HIDING TECHNIQUE

Let [0, M] be image graylevel spectrum (M=255 for eight-bit graylevel images), and let (u, v) be a pair of pixels.

FORWORD TRANSFORM STEP-

For forward transform use below variables

u'=2u-v,

v'=2v-u (1)

For preventing overflow and Under flow policy, the transform is confined to below levels

0<=2u-v<=M (2)

0<= 2v-u<=M

INVERSE TRANSFORM STEP-

Inverse transform procedure is shown by

u= [2/3(u')+1/3(v')] (3)

v= [1/3 (u') + 2/3(v')]

If u' and v' are not swapped, even without the ceil functions, exactly inverts. Using image watermarking technique, the LSBs of u', v' are obscured. Let the LSBs of u' and v' set to "0". It without delay make the LSB of a' was "1," the values in the middle the ceil functions for the summing of u and v decrease with 2/3 and 1/3, respectively. Likewise, if the LSB of v' was "1," the coterminous standards downturn with 1/3 (for the calculation of u) and 2/3 (for the performing arithmetic of v). Omitting when both LSBs are "1," the ceil function recapture the flawless executions. Odd integer number measures by using LSB of "1". From, this measure it tracks that (u', v') are both odd numbers only if (u, v) are odd numbers, too. D be the odd pairs set. Here u'+ v'= u+ v and u'-v'=3(u-v), respectively in this manner. RCM having the graylevel averages. Consequently, image contrast increases is stated here.

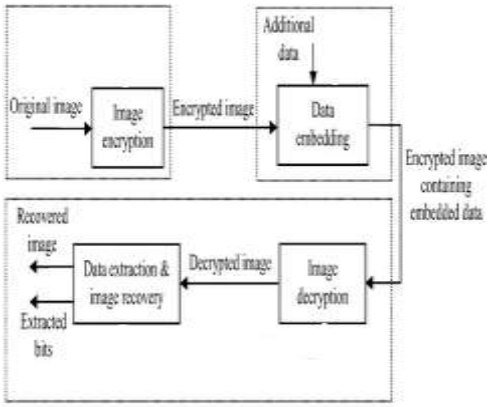

Fig. 1. Flow for embedding and extraction process

IV. INTEGER TRANSFORM MAPPING

At detection of the LSBs we get the, the LSB of the first pixel of exclusive pair is used to manifest if a pair was transformed or not is showing here: "1" for transformed pairs and "0" otherwise described here.

The inverse transform contrast mapping deteriorates to recoup the pair of pixels with odd values like (u, v) $\in$ D. In unmasking procedure, set both the LSBs to "1" and keep account (2). If (2) are delighted, this pair was constituted of odd pixels here. For deflecting decoding uncertainties, certain odd pixel pairs should be phase out, those pairs stationed on the borders of D. The pairs prone to ambiguity are commencing by answering in odd numbers the calculations: 2u-v=1, 2v-u=1,2u-v=M and 2v-u=M. When M=255, then 170 pairs are presented here.

V. INTEGER TRANSFORM FUNCTION

Here entire image divides into pairs of pixels like we can say that (for specimen, on rows, on columns is used here in RCM method).

1) For each pair (u', v') of pixels we go through the following conditions like we can say that here:

a) (u, v) $\in$ D if this is not an adjunct of odd pixel integrity, change this pair by means of the (1), fixed the LSB of u'to "1," and consider the LSB of v' as procurable for data embedding fashion is stated here.

b) If (u, v) $\in$ D and if it is adjunct of odd pixel values, set the LSB of u to "0," and revolve the LSB of v as procurable for data embedding fact is stated here.

c) If, (u, v) $\notin$ D then in this fact fixed the LSB of u to "0," and save the true value for further for consideration here.

VI. STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to

itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Following elements are needed to conceal information into a media which can be any type like text, image etc.:
1) The hidden information in the cover media(C).
2) The text like account number, password, image or any type of data be the Secret message (M).
3) The steganography function (Fg) and its inverse (Fg-1).
Above steganography elements operates as shown in below steganographic operation diagram: -

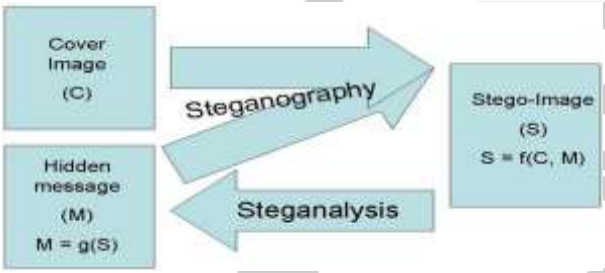

Fig. 2. Steganographic operation

Hiding a secret message into a digital image is most widely technique today. The brightness and Chroma etc. components digitally expressed in terms of 1's and 0's.

Digital image in bitmap format as well as the compressed image format like JPEG, this procedure can be directly applied. The carriers of the unseen messages are the LSB of encoded Discrete Cosine Transformation (DCT) components.

Above procedures details is elaborated in below section: Bitmap format's modification of LSB of a cover image. In this approach, in LSBs of each pixel, binary equivalent of the message. Let's see we will attempt to conceal the character of 'A' into an 8-bit color image.

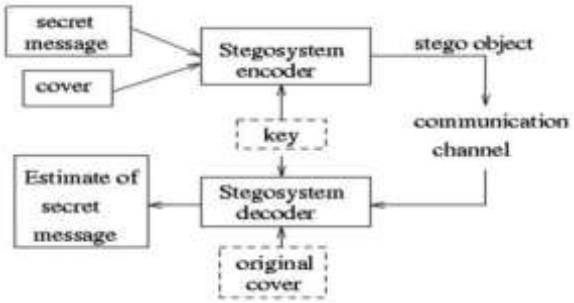

Fig. 3 Basic Steganography model

From top left corner of the image take eight consecutive pixels here. Those pixels equivalent binary bit pattern may be like this we can say: -
00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111
Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern will become like this: -
00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111
While at the discovery end extract the last bit of every pixel to get the equivalent binary impression of unseen data.
Masking procedure can be used to perform this movement. Mask the data with 0x1 so that we can get the last bit of each pixel. The mask procedure is as follows -
00100110& 00000001 = 0
11101001& 00000001 = 1
11001001& 00000001 = 1
00100110& 00000001 = 0
11001000& 00000001 = 0
11101001& 00000001 = 1
11001000& 00000001 = 0
00100111& 00000001 = 1
In this way unseen data 'A' i.e. **01100101** can be extracted. By using steganography method we cannot get the original image pixel values in the decoding procedure so that this method becomes the vulnerable to attacks. But we can get the secret image data as it is. So by comparing Steganography method with the RCM we get best result by using the method RCM.

VII. EXPERIMENTAL WORK

Image quality is measured with metrics which are used in image processing such as PSNR and MSE. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

Fig. 4. Carrier biomedical images sized 512*512

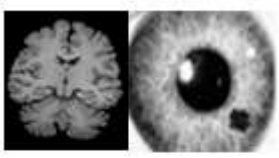

Fig. 5. Secretbiomedical images sized 50*50.

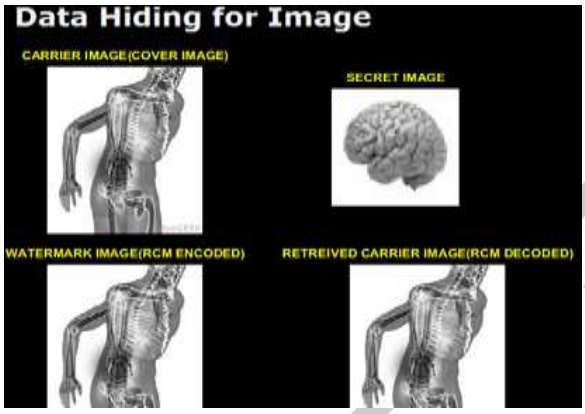

Fig. 6. Encoding process by integer transform method

Images	RCM-PSNR	Stego-PSNR
Heart.tif	100	63.66
Body.tif	98.61	63.05
Brain.gif	99.31	62
CheastXray.gif	99.31	61.69

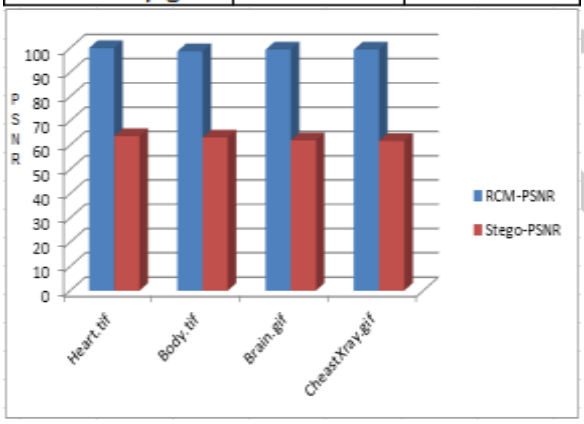

Fig. 7. Comparison of PSNR by using Stegno and RCM method.

The lower the value of MSE, the lower the error. To compute the PSNR, the block first calculates the mean-squared error.

VIII. CONCLUSION

This paper examines a spatial domain reversible watermarking providing high biomedical data or images embedding bit-rate at a very low mathematical complexity. As there is loss in quality of original biomedical image by steganography we propose a Reversible Contrast Mapping (RCM) is a simple integer transform that applies to pairs of pixels. The proposed scheme does not need additional data compression. In Reversible Contrast Mapping there is no loss in quality of original biomedical image. In terms of mathematical complexity, the proposed reversible watermarking appears as being the lowest complexity scheme proposed so far. The computational complexity is reduced for both coding and decoding by using LUT access for each pair of pixels and some low complexity bit manipulation. This makes our scheme very appropriate for real-time applications. Finally, by distributing the location map and by storing the saved true values close to the corresponding pixel pairs, the RCM scheme provides robustness against cropping.

REFERENCES

[1] Gouenou Coatrieux, Wei Pan, Nora Cuppens and Christian Roux, "Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Modification," *IEEE Tran. on Information Security*, vol. 8, pp. 111–120, Jan. 2013.

[2] Dinu Coltuc and Jean-Marc Chassery, "Very Fast Watermarking by Reversible Contrast Mapping", IEEE SIGNAL PROCESSING LETTERS, vol. 14, pp. 255–258, Apr. 2007.

[3] Seung-Won Jung, Le Thanh Ha, and Sung-Jea Ko, "A New Histogram Modification Based Reversible Data Hiding Algorithm Considering the Human Visual System," *IEEE Signal Process. Lett.*, vol. 18, pp. 95–98, Feb. 2012.

[4] Bo Ou, Xiaolong Li, Yao Zhao, Senior Member, Rongrog Ni and Yun-Qing Shi, "Pairewise Prediction-Error Expansion for Efficient Reversible Data Hiding," *IEEE Image Process. Lett.*, vol. 22, pp. 5010–5021, Dec. 2013.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari and Wei Su, "Reversible Data Hiding," *IEEE Trans. Circuits and Video. Lett.*, vol. 16, pp. 354–362, Mar. 2006.

[6] Xinpeng, Shanghai, "Separable Reversible Data Hiding in Encrypted Image," *IEEE Trans. Informaion Forensics. Lett.*, vol. 7, pp. 826–832, Apr. 2012.

[7] Lingling An, Xinbo Gao, Xuelong Li, Dacheng Tao, Cheng Deng and Jie Li, "Reversible Data Hiding," *IEEE Transactions on image processing.*, vol. 21, pp. 3598–3611, Aug. 2012.

[8] S.Z.Wang, X.P.Zhang, "Recent advance in image-based steganalysis research," Chinese journal of computers,vol. 32,pp. 1247-1263,July 2009.

[9] I. Avcibas, N. D. Memon, "Steganalysis using image quality metrics,"IEEE Trans Image Process, vol,12, pp. 221-229,2003.

[10] A.Yadollahpour, H. M. Naimi, "Attack on LSB steganography in color and grayscale images using autocorrelation coefficients," European Journal of Science Research,vol.31,pp. 172-183,Feburary 2009