e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Optimized Reversible Data Hiding Technique for Secured Data Transmission

Ms. P. Umamaheswari[1], Dr. S. Sathappan[2], Mr. R. Subramanian[3]
[1]*Research Scholar,*
[2]*M.Sc., PGDCA., M.Phil., Ph.D., Associate Professor of Computer Science,*
[1,2]*Department of Computer Science, Erode Arts and Science College (Autonomous), Erode., TN, India*
[3]*Erode Arts College, Erode*

Abstract-Reversible data hiding (RDH) is used to embed secret message into a cover image by slightly modifying its pixel values. Embedded message and the cover image are completely recovered from the marked content. RDH supports information hiding with the lossless compressibility of natural images. Lossless compression, difference expansion, histogram modification, prediction-error expansion and integer transform techniques are used for RDH process. Histogram based RDH method is divided into two steps histogram generation and histogram modification. Histogram construction is performed with the pixel pairs sequences and their different values. Histogram modification is carried out to embed data into the cover image. The un-hiding process recovers the message and also the cover image.

Reversible data hiding (RDH) scheme is designed by using difference-pair-mapping (DPM) mechanism. A sequence consisting of pairs of difference values is computed by considering each pixel-pair and its context. DPM is an injective mapping defined on difference-pairs. Specifically designed DPM is used for Reversible data embedding process. A two-dimensional difference-histogram is generated by counting the frequency of the resulting difference-pairs. Current histogram-based RDH methods use natural extension of expansion embedding and shifting techniques. A pixel-pair-selection strategy is adopted to use the pixel-pairs located in smooth image regions to embed data. Capacity distortion property is used evaluate the embedding capacity (EC).

Two dimensional difference histogram modification model is enhanced to increase the embedding capacity. Difference Pair Mapping (DPM) model is optimized to identify pixel redundancy. Multiple in value based pixel pair modification is allowed in the system. Histogram modification is carried out with different frequency levels.

I. INTRODUCTION

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word steganography combines the Ancient Greekwords steganos, meaning "covered, concealed, or protected", and graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be something else: images, articles, shopping lists, or some other cover text [1]. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. 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 [10]. 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.

Reversible data hiding is capable of restoring the original image at the data extracting stage; therefore, the embedding methods of this type are useful at some applications such as military or law enforcement, where the original images are demanded. In 2003, Tian proposed a reversible data hiding method based on difference expansion. They partitioned the cover image into pixel pairs and embedded a message bit into the LSB of the expanded difference. Tian's method provides high payload, the distortion caused by difference expansion is significant. Ni et al. in 2006 proposed a very different reversible approach to embed data by using the histogram-shifting method. In their method, histogram bins are shifted to vacate an empty bin for data embedment. Ni et al.'s method provides an excellent image quality; the payload is limited by the peak height of the image histogram. In 2007, Thodi and Rodriguez combined the difference expansion and histogram shifting methods and proposed a new embedding method to achieve reversibility. Thodi and Rodriguez's method significantly reduces the distortion caused by difference expansion while providing a very satisfactory payload.

II. RELATED WORKS

To well exploit the redundancy of natural images, the difference- histogram-based RDH methods utilize pixel-pairs with small differences for expansion embedding and other pairs for shifting. These methods may control the maximum modification to each pixel value and thus the marked image quality can be well guaranteed. There are several related works providing valuable thoughts [2]. In 2006, Lee *et al.* proposed a difference-histogram based RDH method. The method modifies the pixel-pairs with differences 1 or -1 to carry data. Specifically, for data embedding, the difference image is first computed for a gray-scale cover image I as (1) w

$$D(i,j) = I(i, 2j + 1) - I(i, 2j) \quad (1)$$

where (I(i,2j), I(i, 2j + 1)is a pixel-pair consisting of two consecutive pixels. Then the marked image I^m can be obtained as

$$I^m(i,2j+1) = \begin{cases} I(i,2j+1). & if\ D(i,j) = 0 \\ I(i,2j+1) + b. & if\ D(i,j) = 1 \\ I(i,2j+1) + b. & if\ D(i,j) = -1 \\ I(i,2j+1) + 1 & if\ D(i,j) \geq 2 \\ I(i,2j+1) - 1 & if\ D(i,j) \leq -2 \end{cases} \quad (2)$$

where b ∈ {0,1}is a data bit to be embedded. Notice that the first pixel I(i,2j)in the pair keeps unchanged in this embedding procedure, i.e., one simply takes I^m(i,2j), I(i, 2j). Accordingly, from a marked image, the embedded data bit can be extracted as

$$b = \begin{cases} 0, & if\ D^m(i,j) = \pm 1 \\ 1, & if\ D^m(i,j) = \pm 2 \end{cases} \quad (3)$$

and the original pixel value can be recovered as

$$I(i,2j+1) = \begin{cases} I^m(i,2j+1). & if\ D^m(i,j) = 0 \\ I^m(i,2j+1) + -1. & if\ ID^m(i,j) \geq 2 \\ I^m(i,2j+1) + 1 & if\ D(i,j) \geq -2 \end{cases} \quad (4)$$

where is the difference $D^m(i,j) = I^m(i,2j+1) - I^m$ (i, 2j) is the difference value computed from the marked image.

In this method, the bins 1 and -1 are utilized for expansion embedding and other bins for shifting. It outperforms some classical RDH methods. In 2009, another difference-histogram-based RDH method was proposed by Tai *et al.* [8]. Recently, Tai *et al.*'s method is improved by Hong [9] by utilizing a dual binary tree (DBT), a better pixel predictor and an error energy estimator. Compared with Tai *et al.*'s, Hong's DBT-based method can increase EC at the same level of distortion. Experimental results demonstrate that Hong's method can significantly improve the image quality and EC of Tai *et al.*'s and some state-of-the-art works. It is worth mentioning that some recent works [3] can also be viewed as Tai *et al.*'s improvement. The difference value is replaced by the prediction-error computed using a larger local image region so that the redundancy can be better exploited. Our method is motivated by the aforementioned works and will be described in details.

III. REVERSIBLE DATA HIDING SCHEME AND ITS ISSUES

Reversible data hiding (RDH) aims to embed secret message into a cover image by slightly modifying its pixel values, and, unlike conventional data hiding, the embedded message as well as the cover image should be completely recovered from the marked content [5]. RDH is a special type of information hiding and its feasibility is mainly due to the lossless compressibility of natural images. The reversibility in RDH is quite desirable and helpful in some practical applications such as medical image processing [7], multimedia archive management, image trans-coding and video error-concealment coding [4], etc. Generally, the performance of a RDH scheme is evaluated by the capacity-distortion behavior. For a required embedding capacity (EC), to obtain a good marked image quality, one expects to reduce the embedding distortion as much as possible. Many RDH methods have been proposed so far, e.g., the methods based on lossless compression, difference expansion[8], histogram modification [3], prediction-error expansion and integer transform, etc. Among them, the histogram-based ones have attracted much attention. The histogram-based methods modify the histogram in such a way that certain bins are shifted to create vacant space while some other bins are utilized to carry data by filling the vacant space. This type of methods can well control the embedding distortion and provide a sufficient EC.

The first histogram-based RDH method is the one proposed by Ni *et al.*. This method uses peak and minimum points of the pixel-intensity-histogram to embed data. It changes each pixel value at most by 1 and thus a good marked image quality can be obtained [6]. Its EC is quite low and this method does not work well if the cover image has a flat histogram. To facilitate it, Lee *et al.* proposed to utilize the difference-histogram instead. This novel method exploits the correlation among neighboring pixels and can embed larger payload with reduced distortion compared with Ni *et al.*'s. Moreover, we will see later that Lee *et al.*'s method can be in fact implemented, in an equivalent way, by modifying the two-dimensional pixel-intensity-histogram according to a pixel-pair-mapping (PPM) which is an injective mapping defined on pixel-pairs. In this light, the superiority of Lee *et al.*'s method over Ni *et al.*'s is explained in another viewpoint. Afterwards, Fallahpour introduced a method by modifying the histogram of prediction-error. Like difference-histogram, the prediction-error-histogram is also Laplacian-like and sharply distributed which guarantees an excellent embedding performance. Instead of only using the correlation of two adjacent pixels in Lee *et al.*'s method, Fallahpour's method can exploit the local correlation of a larger neighborhood, and thus can provide relatively better performance. Besides the aforementioned methods, many other works are also based on histogram by incorporating some strategies such as double-layered embedding, embedding-position-selection [9], adaptive embedding, context-modification and optimal-bins-selection, etc.

Reversible data hiding (RDH) scheme is designed by using difference-pair-mapping (DPM) mechanism. A sequence consisting of pairs of difference values is computed by considering each pixel-pair and its context. DPM is an injective mapping defined on difference-pairs. Specifically designed

DPM is used for Reversible data embedding process. A two-dimensional difference-histogram is generated by counting the frequency of the resulting difference-pairs. Current histogram-based RDH methods use natural extension of expansion embedding and shifting techniques. A pixel-pair-selection strategy is adopted to use the pixel-pairs located in smooth image regions to embed data. Capacity distortion property is used evaluate the embedding capacity (EC). The following drawbacks are identified in the current reversible hiding scheme. They are Embedding capacity (EC) is low, Difference Pair Mapping (DPM) is not optimized, Limited embedding performance in the DPM model and two dimensional histogram utilization is low.

IV. TWO-DIMENSIONAL HISTROGRAM MODIFICATION MECHANISM

4.1. PPM for RDH

We point out that, in an equivalent way, Lee *et al.*'s embedding procedure can be demonstrated by a PPM, in which a subset of $\mathbb{Z}^2$is divided into two disjointed parts as black points and blue points, each black point is mapped to a blue one and each blue point is mapped to another blue point. Here, each point represents the value of a pixel-pair, and the black points are used for expansion embedding while the blue ones for shifting. According to this PPM, for a cover pixel-pair (x, y), its marked value can be determined in the following way:

1) if y – x = 0 (i.e., (x,y)is a red point), the marked pixel-pair is taken as (x, y) itself.
2) if yy-x = 1or y-x = -1
- if the to-be-embedded data bit , the marked pixel-pair is taken as (x, y) itself.
- if the to-be-embedded data bit b = 1, the marked pixel-pair is taken as its associate blue point.

3) if y – x > 1 or y – x < -1, the marked pixel-pair is taken as its associate blue point.

4.2. DPM for RDH

For a pixel-pair, we propose to compute two difference values d_1= x – y and d_2 = y –z and to form a two-dimensional difference-histogram of (d_1, d_2), where is a prediction of which will be clarified later. Inspired by the aforementioned new PPM, we will modify either x or y by 1. In this situation, since (x, y) has four modification directions, the difference-pair (d_1, d_2) also has four modification directions: (d_1-1, d_2), (d_1+ 1, d_2), (d_1+ 1, d_2 -1) or (d_1- 1, d_2+ 1). Based on these four modification directions, we will introduce a new RDH scheme by designing a DPM. For each pixel-pair (x, y), compute the prediction of y to z get using GAP predictor:

$$z = \begin{cases} v_1, & \text{if } d_v - d_h > 80 \\ \frac{(v_1+u)}{2}, & \text{if } d_v - d_h \in (32, 80] \\ \frac{(v_1+3u)}{4}, & \text{if } d_v - d_h \in (8, 32] \\ u, & \text{if } d_v - d_h \in [-8, 8] \\ \frac{(v_4+3u)}{4}, & \text{if } d_v - d_h \in [-32, 8) \\ \frac{(v_4+u)}{2}, & \text{if } d_v - d_h \in [-80, -32) \\ v_4, & \text{if } d_v - d_h < -80 \end{cases} \quad (5)$$

where {v_1,……v_5,v_7,v_8}are neighboring pixels of (x, y), $d_v = |v_1 - v_5| + |v_3 - v_7| + |v_4 - v_8|$ and $d_h = |v_1 - v_2| + |v_3 - v_4| + |v_4 - v_5|$ represent the vertical and horizontal gradients, and $u = (v_1 + v_4)/2 + (v_3 - v_5)/4$. Notice that z should be rounded to its nearest integer if it is not an integer. Then, compute the noisy-level (x, y) of denoted as NL (x, y) using its ten neighboring pixels {v_1,……..,v_{10}}as

$$NL(x, y) = \int_{(i',j')\in V} |\nabla I(i', j')| \quad (6)$$

where V represents the context of (x, y) containing the ten pixels and stands for the gradient operator.

4.3. Data Embedding and Extraction Procedures

The proposed data embedding procedure contains several basic steps. First, divide the cover image into non overlapping pixel-pairs. Then, embed the secret message into a part of cover image. Next, record the least significant bits (LSB) of some pixels of I' to get a binary sequence, and embed this sequence into the rest part of I, i.e., I – I'. Finally, by using LSB replacement, embed the auxiliary information and the compressed location map into I''. The detailed data embedding procedure is described as bellow step-by-step.

4.4. RSA Algorithm

The domain name service sensitive attributes are secured using the RSA algorithm. The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Key Generation

Select p,q	p and q both prime , $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1; 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Cipher text	$C = M^e \pmod n$

Decryption

Cipher text	C
Plaintext	$M = C^d \pmod n$

V. INTEGRATION OF REVERSIBLE DATA HIDING SCHEME WITH CRYPTOGRAPHY

Two dimensional difference histogram modification model is enhanced to increase the embedding capacity. Difference Pair Mapping (DPM) model is optimized to identify pixel redundancy. Multiple in value based pixel pair modification is allowed in the system. Histogram modification is carried out with different frequency levels. The system is divided into four major modules. They are sender, data security, receiver and data retrieval. The sender module is designed to send the image data values. Data security is designed to perform hiding and encryption process. Data receiver module collects data form the sender. Data extraction module is designed to perform unhide operations.

The data sender collects secret data and cover data from the user. Histogram construction is carried out using the cover data image. Secret data is converted into bits. Data security process is used to hide secret data values. RSA algorithm is used to encrypt the data values. Encrypted data values are hided in the cover image. Data receiver collects data from the sender node. Received data values are updated into the local l memory. Data receiver fetches the key value from the sender. Secret data is separated from the received data values. Cover data is also separated from the received data values. Decryption process is carried out to fetch the secret data.

5.1. Sender

The data sender collects secret data and cover data from the user. Pixel Pair Mapping (PPM) and Difference Pair Mapping (DPM) techniques are used in the system. Difference Pair Mapping is

optimized to construct histograms. Histogram construction is carried out using the cover data image. Secret data is converted into bits.

5.2. Data Security

Data security process is used to hide secret data values. RSA algorithm is used to encrypt the data values. The sender collects the public from the receiver node for the encryption process. Encrypted data values are hided in the cover image.

5.3. Receiver

Data receiver collects data from the sender node. Received data values are updated into the local memory. The received data value is passed to the unhide and decrypt process. The receiver node maintains the secret key for decryption process.

5.4. Data Extraction

Secret data is separated from the received data values. Cover data is also separated from the received data values. Decryption process is carried out to fetch the secret data. Cover data quality is analyzed with image quality measures.

VI. PERFORMANCE ANALYSIS

The Reversible Data Hiding (RDH) scheme is improved with Cryptography techniques and optimal difference pair mapping process. The secret text values are embedded in the cover image under the encoding process. The secret text is encrypted before the encoding process. The RSA algorithm is used for the encryption and decryption process. The decryption process is carried out after the decoding process. The system is designed as sender and receiver application. The encryption and encoding operations are performed in the sender application. The decoding and decryption operations are carried out under the receiver process. The sender transforms the embedded image to the receiver. The receiver decodes the image and extracts the secret text.

The secured data transmission system is tested with sender and receiver application. Reversible Data Hiding with Difference Pair Mapping (RDH-DPM) model and Reversible Data Hiding with Optimized Difference Pair Mapping (RDH-ODPM) models are used in the system. The RDH-DPM model performs the data hiding on histogram points. The RDH-ODPM model performs the data hiding process on optimized DPM positions. The system selects the threshold for the histogram dynamically. The RDH-ODPM scheme also uses the encrypted message for the hiding process. The system is tested with different set of data transmission cycles. The system performance is measured with three parameters. They are Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Embedding Capacity (EC) metrics. The PSNR and MSE metrics are used to evaluate the received image quality. The hiding capacity is analyzed using the embedding capacity measure.

6.1. Peak Signal-to-Noise Ratio (PSNR)

The image quality is analyzed using Peak Signal-to-Noise Ratio (PSNR) method. Peak Signal-to-Noise Ratio is the ratio between the reference signal and the distortion signal in an image, given in decibels. The higher the PSNR, the closer the distorted image is to the original. In general, a higher PSNR value should correlate to a higher quality image, but tests have shown that this isn't always the case. PSNR is a popular quality metric because it's easy and fast to calculate while still giving okay results. For images $A = \{a_1 .. a_M\}$, $B = \{b_1 .. b_M\}$ and MAX equal to the maximum possible pixel value:

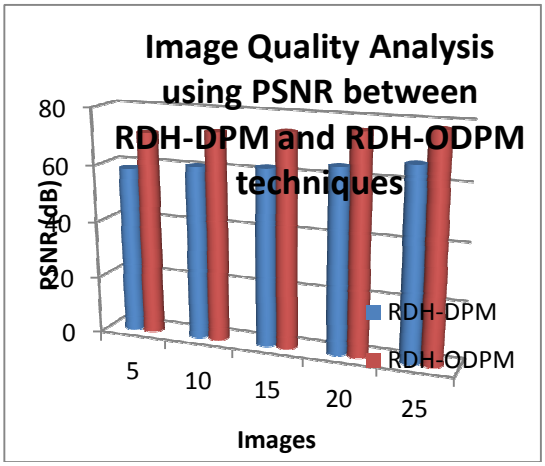

Figure No.6.1. Image Quality Analysis using PSNR between RDH-DPM and RDH-ODPM Techniques

$$PSNR(A,B) = 10log_{10}\left(\frac{MAX^2}{MSE(A,B)}\right)$$

The Reversible Data Hiding with Difference Pair Mapping (RDH-DPM) scheme and Reversible Data Hiding with Optimized Difference Pair Mapping (RDH-ODPM) scheme are tested using Peak Signal to Noise Ratio (PSNR) metric for image quality analysis in receiver end. PSNR analysis is shown in figure 6.1. The analysis shows that the PSNR in RDH-ODPM is 15% increased than the RDH-DPM method.

6.2. Mean Squared Error (MSE)

The image quality analysis for the data hiding and transmission process is performed using the Mean Square Error (MSE) metric. Mean Squared Error is the average squared difference between a reference image and a distorted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. For images A = $\{a_1 .. a_M\}$ and B = $\{b_1 .. b_M\}$, where M is the number of pixels:

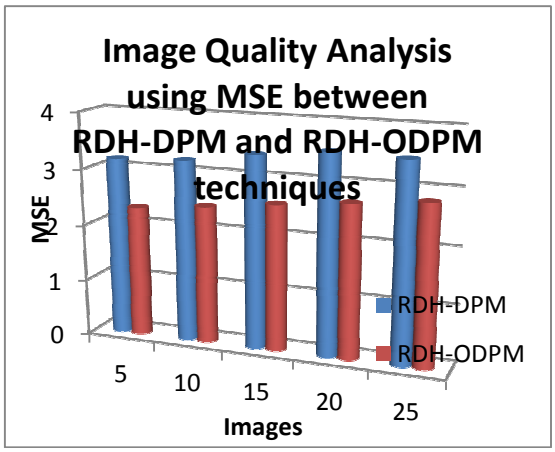

Figure No. 6.2. Image Quality Analysis using MSE between RDH-DPM and RDH-ODPM Techniques

$$MSE(A,B) = \frac{1}{m}\sum_{i=1}^{M}(a_i - b_i)^2$$

The squaring of the differences dampens small differences between the 2 pixels but penalizes large ones. The Reversible Data Hiding

with Difference Pair Mapping (RDH-DPM) scheme and Reversible Data Hiding with Optimized Difference Pair Mapping (RDH-ODPM) scheme are tested using Mean Square Error (MSE) metric for image quality analysis in receiver end. MSE analysis is shown in figure 6.2. The analysis shows that the MSE in RDH-ODPM is 25% reduced than the RDH-DPM.

6.3. Embedding Capacity (EC)

The performance of data hiding schemes is verified with Embedding Capacity (EC) parameter. Embedding Capacity is used to represent the amount of data that can be hided in the cover image. The embedding capacity is estimated with the possible pixel count that can be obtained for the hiding process. In the Reversible Data Hiding (RDH) scheme the pixels that are selected for the hiding process is denoted as embedding capacity. The pixel selection is performed with the histogram analysis mechanism. The Reversible Data Hiding with Difference Pair Mapping (RDH-DPM) scheme uses the fixed threshold for the pixel selection process. The Reversible Data Hiding with Optimal Difference Pair Mapping (RDH-ODPM) scheme uses the dynamic threshold value for the hiding process.

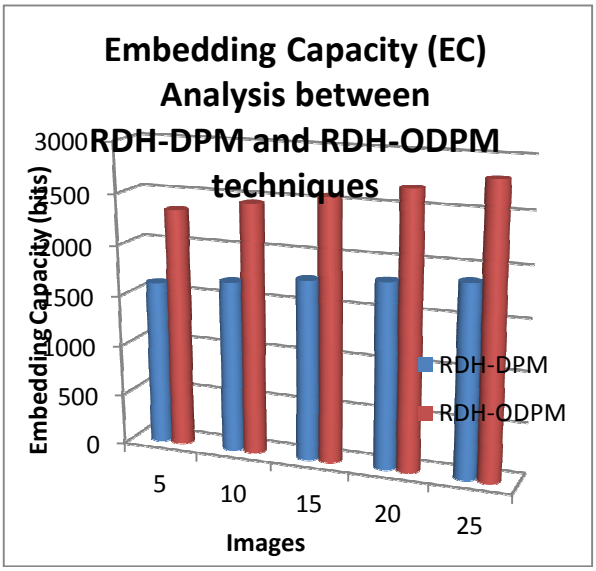

Figure No. 6.3. Embedding Capacity (EC) Analysis between RDH-DPM and RDH-ODPM Techniques

The Reversible Data Hiding with Difference Pair Mapping (RDH-DPM) scheme and Reversible Data Hiding with Optimized Difference Pair Mapping (RDH-ODPM) scheme are tested using Embedding Capacity (EC) parameter for hiding performance analysis. Embedding Capacity (EC) parameter analysis is shown in figure 6.3. The analysis shows that the embedding capacity in RDH-ODPM is 30% improved than the RDH-DPM.

VI. CONCLUSION AND FUTURE WORK

Reversible Data Hiding (RDH) techniques are used to support data hiding with message and cover image retrieval mechanism. Difference Pair Mapping (DPM) model is used for histogram construction process. Two dimensional difference histogram modification method is used for the data hiding process. The system is enhanced to improve the embedding capacity with optimized DPM. Embedding performance is improved by the system. The system reduces the capacity distortion in hiding process. The system supports efficient coverage image retrieval process. The system reduces the process time in hiding and un-hiding process.

- The reversible data hiding scheme based data distribution system can be enhanced with data integrity techniques to verify the data transfer process.
- The system can be improved to support intrusion detection process.
- The data hiding process can be applied on other cover data mediums such as audit and video files.

REFERENCES

[1] Bin Li, Shunquan Tan, Ming Wang and Jiwu Huang, "Investigation on Cost Assignment in Spatial Image Steganography", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 8, August 2014.
[2] Chuan Qin, Chin-Chen Chang and Yi-Ping Chiu, "A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting", IEEE Transactions On Image Processing, Vol. 23, No. 3, March 2014
[3] W. Hong and C. W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," J. Syst. Software, Nov. 2009.
[4] K.-L. Chung and H.-Y. Liao, "Reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," IEEE Trans. Circuits Syst. Video Technol., Nov. 2010.
[5] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," EURASIP J. Inf. Security, vol. 2010, 2010.
[6] Xiaolong and Bin Yang, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification", IEEE Transactions on Information Forensics and Security, July 2013.
[7] M. Fontani and M. Consalvo, "Reversible watermarking for image integrity verification in hierarchical pacs," in Proc. 12th ACM Workshop on Multimedia and Security, 2010.
[8] W. L. Tai, C. M. Yeh and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., Jun. 2009.
[9] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," Opt. Commun., 2012.
[10] Dawen Xu, Rangding Wang and Yun Q. Shi, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

