A Novel Method of Secure Communication through Randomized Pixel Variation (RPV)

M.Thanga kavitha, S.Sangeetha, N.Manikandaprabu

Abstract— A Novel Reversible Data Hiding Scheme (RDH) using Randomized Pixel Variation (RPV) is proposed here. It is based on the biological process of controlling the color of the epithelial tissue by a pigment cell, named as melanocyte. The pixel pair mapping technique is utilized to select the pixel randomly to hide the data bit. The main objective of this work is to satisfy robustness, imperceptibility and high capacity simultaneously. A new informed image watermarking scheme with a simplified complexity of 1.511x10-3sec and an information rate of 1/150 bit/pixel is obtained. While comparing the proposed approach with conventional method, the image redundancy is exploited, thereby embedding performance is improved. Due to slight variation in the pixel values, the high image quality is preserved. The performance is analyzed using Peak Signal to Noise Ratio (PSNR) calculations and Structural Similarity (SSIM) index for watermark imperceptibility and robustness, respectively. The Experimental results show that the value of PSNR and SSIM is 72.95 dB and 1.00, respectively.

Index Terms— Data hiding, Location Map, Pixel pair mapping, Randomized Pixel Variation, Reversible watermarking.

1 INTRODUCTION

Digital watermarking is a kind of data hiding technology. Its basic idea is to embed covert information into a digital signal, like digital audio, image, or video, to trace ownership or protect privacy. Among different kinds of digital watermarking schemes, reversible watermarking has become a research hotspot recently. Compared with traditional watermarking, it can restore the original cover media through the watermark extracting process; thus, reversible watermarking is very useful, especially in applications dictating high fidelity of multimedia content, such as military aerial intelligence gathering, medical records, and management of multimedia information.

The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various software products have been recently introduced in attempt to address these growing concerns. It should be possible to hide data (information) within digital audio, images and video files. The information is hidden in the sense that it is perceptually and statistically undetectable. One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called digital signature or copyright label or watermark, which completely characterizes the person who applies it and, therefore, marks it as being his intellectual property.

Chih-Chin Lai et al.[1] developed an image watermarking technique to satisfy both imperceptibility and robustness requirements. It is accomplished by the combination of a hybrid image-watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD), where the PSNR of the watermarked image is 51.14 dB.

Chuntao Wang et al. [2] developed a new informed image watermarking scheme with high robustness and simplified complexity at an information rate of 1/64 bit/pixel. It uses the Taylor series approximated locally optimum test (TLOT) detector based on the hidden Markov model (HMM) in the wavelet domain. The process of informed embedding is formulated as an optimization problem under the robustness and distortion constraints and the genetic algorithm (GA) is then employed to solve this problem. Simulation results demonstrate that it has high robustness against common attacks in signal processing with a greatly reduced arithmetic complexity. The PSNR of the watermarked image is between 36-38 dB.

Dimitrios Simitopoulos et al. [3] proposed a robust image watermarking based on generalized random transformations. It is based on the properties of the RIT (Radial Integration Transform) and CIT (circular integration transform) generalized Radon transformations and manages to synchronize the watermark that is embedded in an image with the correlating watermark in case of geometric attacks. It is able to withstand a variety of attacks including common geometric attacks but the PSNR of the watermarked image is 41.76 dB. Dong Zheng et al. (2009) developed a watermarking scheme based on rotation invariant feature and image normalization. A mathematical model is established to approximate the image based on the mixture generalized Gaussian distribution, which can facilitate the analysis of the watermarking processes but the PSNR of the watermarked image is 40.089 dB.

Recently, Mohammad Ali Akhaee et al. [12] developed a robust image watermarking scheme based on a sample projection approach. It uses the low-frequency components of image blocks for data hiding to obtain high robustness against attacks. It uses four samples of the approximation coefficients of the image blocks to construct a line segment in the 2-D space. The slope of this line segment, which is invariant to the gain factor, is employed for watermarking purpose. It embeds the watermarking code by projecting the line segment on some specific lines according to message bits. The watermark invisibility is perfectly satisfied with the PSNR around 40.39 dB. To quantitatively evaluate the imperceptibility of the watermarked images, it use the mean structural similarity index (MSSIM) whose

- *M.Thanga kavitha and S.Sangeetha are currently pursuing master degree program in Applied Electronics in Akshaya College of Engineering and Technology,TamilNadu,India, PH- +91-9677552968 and 9677881555.Email: thangakavitha90@gmail.com and Sangeethashanmugam09@gmail.com*
- *N.Manikandaprabu, is currently working as a lecture in Electronics and Communication Engineering in Senthur Polytechnic College, TamilNadu, India, PH- +91-9150061808. E-mail: manikandaprabube@gmail.com*

value is 0.9984.

2 DESIGN METHODOLOGY

Life is the most fascinating thing of the universe. Of all life, the human being is the highest evolved creature with a most complicated life form. The human body is complex and amazing machine. It is an intricate collection of millions of cell which form tissues, organs, and organ system of the body. A cell is the structural and functional unit of the body and performs a lot of functional unit of the body and performs a lot of function. The cells are very complicated structure. It is a microscopic factory where thousands of chemical reactions are carried out in a controlled way. A group of similar cells join to form a tissue to carry out some specialized functions of the body. Skin is an epithelial tissue. In adult body, there are over a hundred million cells of different types ranging differently in size. The cells are different because they have to do different jobs in different parts of the body. Cell, though differ markedly in shape, size, color, and function, they are basically similar. The difference in the color of the skin is due partly to the amount of blood circulating through the dermis and the texture of the dermis.

A man becomes white with fear because in fear small vessels close off, red with anger because of increased blood flow, and blue with cold because the oxygen moves out from the blood into the tissues as the flow slows down. Apart from this, the color of skin is mainly due to presence of coloring pigment, melanin. Melanin is blackish brown substance found in the deep epidermis. This pigment cell is named as melanocyte. Irrespective of the race, the numbers of melanocytes present in the skin are same. Melanins protect the skin from harmful radiation of the sun. The algorithm developed is analogous to this biological process. The cell is mapped to the pixel of the image. The melanocyte is mapped to the location map which is used to hide the data bit in the image.

The technique RPV is based on modification of two-dimensional difference-histogram by constructing a DPM which is an injective mapping defined on difference-pairs and it is a natural extension of expansion embedding and shifting technology. A pixel pair selection strategy is adopted in this novel method to priority use the pixel pairs located in smooth image regions to embed data. The image redundancy can be better exploited by this approach .this novel method exploits the correlation among neighboring pixels with reduced distortion. Pixel pair mapping (PPM) which is the injective mapping defined on pixel pairs. For the proposed method, by considering a pixel pair and context, a local image region is projected to a 2D space to obtain a sequence consisting of difference pairs. In this technique, the bins 1 and -1 are utilized for expansion embedding. Finally, reversible data embedding is implemented according to a specifically designed difference pair mapping (DPM).

2.1 MIGRATION OF EMBEDDING CAPACITY

Using the Proposed technology, there is a slight variation in the pixel range. The pay load capacity is fixed to 7000 bits and so there is 0.392% variation in the selective single pixel. The maximum data bits can be embedded without degrading the high image quality.

The figure.1 represents the migration of the secret data that has to be embedded in the cover image. The data relevant to the image is first migrated by certain limit. Since

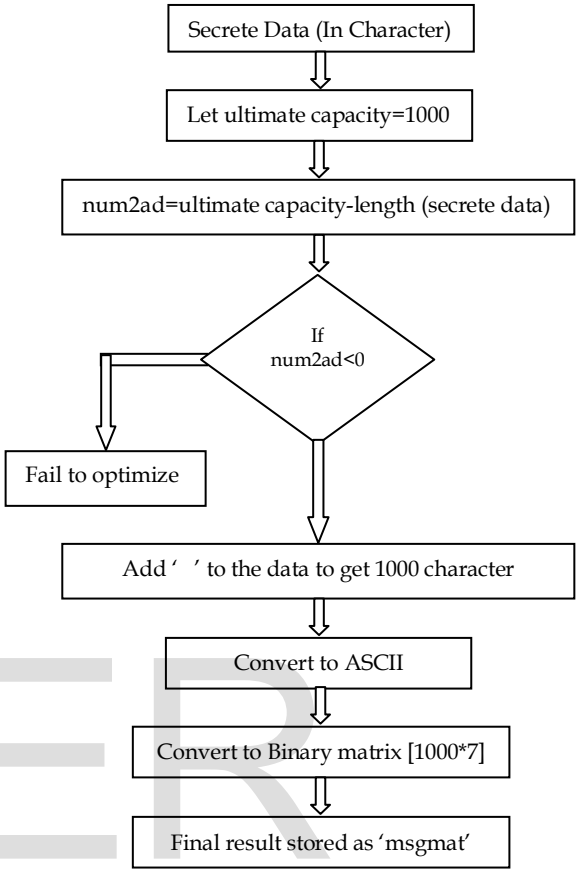


Fig. 1.Migration of Embedding Capacity

it is pointed out that an Embedding Capacity of 3,500 bits is enough for the application of RDH in military application, medical image sharing etc., so the threshold value for optimization is set as 1,000 Characters (7,000 bits).

If the length of character is above the threshold value, the embedding process will be failed. The migration is done by padding the null character to the payload which has the length less than the threshold value.

Further the processing is initialized by converting the character to its corresponding ASCII values which has exactly 1000 values. In MATLAB, whatever the data (character, audio, image, video, etc.,) may be, it can be processed in matrix format. So it is then converted to the matrix form which has the value 1 and 0.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ & & & \vdots & & & \\ & & & \vdots & & & \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{1000\times 7}$$

Fig.2. The resultant value of the Migration process

2.2 TO DETERMINE THE SIZE OF LOCATION MAP

The selected cover image is preprocessed to obtain the grayscale image whose pixel intensity value ranges from 0 to 255. These help to reduce the computational complexity. Additionally the size of image is calculated from which the parameter 'dim1' and 'dim2' is evaluated as mentioned in the equation (1), (2)

$$dim1 = piclngth\text{-}m \quad \ldots (1)$$

$$dim2 = pichghht\text{-}n \quad \ldots (2)$$

Where piclngth, pichghht are the number of the rows and columns of the pixels in the cover image. The value m, n should be small as possible so that the size of LM is comparatively smaller than the size of cover image.

It forms the basis of the determination of the pixel pair mapping (i.e.) size of the location map. Additionally, the key is imported to vary pass for finding the points in the location map for both embedding and extracting the data bit.

2.3 PIXEL PAIR MAPPING ALGORITHM

The algorithm developed to determine the pixel pair mapping is shown in the fig.4. It can also be termed as the mask pattern which is analogous to the biological process. This is a matrix for finding the points to hide the message.

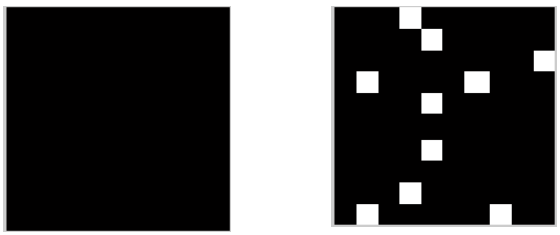


Fig. 3. A zero matrix of size 10×10 and the resultant matrix to hide the data

The input of this algorithm is rows, columns, dim1, dim2, and key. The rows and column are used to indicate the exact point of the location map. The dim1 and dim2 are used to determine the size of the mask pattern. Initially the zero matrix 'A' is defined which is nothing but the mask pattern. The iteration of this algorithm will be repeated for 7,000 times to get 7,000 points in the location map. The variables row and column are used for 2 purpose: one for robustness (i.e.) to transmit the data bit securely and another one is to make decision on the mapping of the point in the location map. It resembles the hole where the data bit can be stored efficiently.

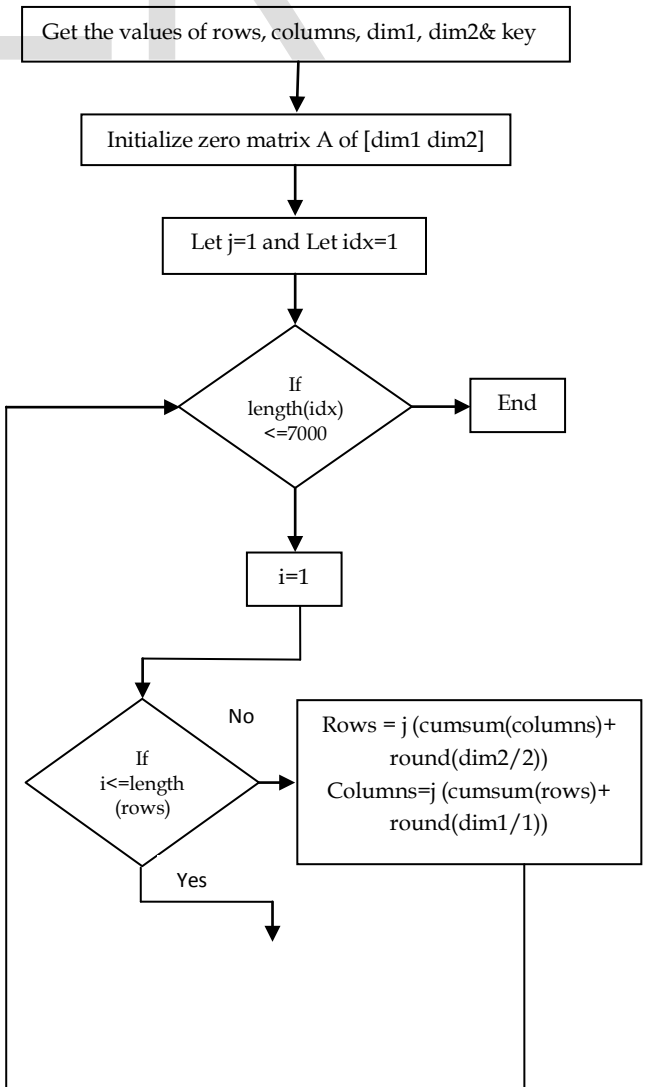
For simplicity, the zero matrix of size 10×10 is selected as the mask pattern and algorithm is performed to get the resultant matrix at the right side of fig 3. The white block, which represents the position where the data bit going to be embed in the corresponding position of the cover image.

After secret messages are embedded, some overhead information is needed to extract the covert information and restore the original image. Generally, the overhead information contains the following:

1) The information to identify those pixels containing embedded bits.

2) The information to solve the overflow/underflow problem. In our proposed scheme, we use four keys to identify the pixels containing embedded bits, and exploit a boundary map, to record information on solving the overflow/underflow problem.

When a boundary pixel is encountered during the extracting process, it is originally either a boundary pixel or a pseudo boundary pixel. Therefore, to find the original boundary pixels, we only need to tell whether boundary pixels in the watermarked image are genuine or pseudo. A boundary map is the right judge to distinguish between genuine and pseudo. It is a binary array with its every element corresponding to a boundary pixel in the watermarked image, 0 for genuine and 1 for pseudo.



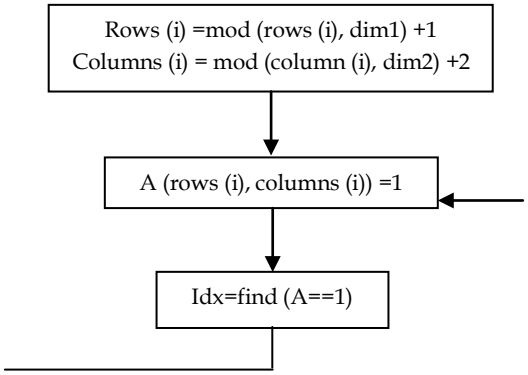


Fig.4. Flowchart of the proposed technique

2.4 EMBEDDING PROCESS

According to Randomized pixel variation scheme, the algorithm is developed as follows:

1. If the pixel pair in the location map (LM) is 0, the marked pixel pair is taken as itself.
2. If the pixel pair in the location map is 1,
   a. If the remainder of division of pixel pair in the cover image by 2 is 0 and the to-be-embedded data bit is 1, then the pixel in the cover image is incremented by one.
   b. If the remainder of division of pixel pair in the cover image by 2 is 1 and the to-be-embedded data bit is 0, then the pixel in the cover image is decremented by one.

2.5 EXTRACTION PROCESS

The corresponding data extraction and image restoration process are summarized as follows:

The reverse operations take place where the complexity lies in finding the bit 1 of the message. This also depends on the location map where the same pixel pair mapping algorithm is utilized. In embedding process, the value of pixel is even before the operation take place. After the selection of the pixel to hide the data, it will be incremented to one. It implies the representation of odd value and the pixel value is selected to restore the secret message in this extraction process.

3. EXPERIMENTAL RESULTS

To analyze the performance of the proposed method in terms of watermark imperceptibility of the watermarked image using PSNR calculations and watermark robustness of the extracted watermark using SSIM index.

The Root Mean Square Error (RMSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image reconstruction quality. The RMSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of RMSE, which represents the error reduction.

$$\mathrm{RMSE} = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[\tilde{f}(m,n) - f(m,n)]^2} \qquad \ldots (3)$$

The PSNR 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.

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{I_{MAX}}{\mathrm{RMSE}}\right) \qquad \ldots (4)$$

Where I_{MAX} is the maximum gray level of the image. In this case, I_{MAX} is the maximum value of 255.

$$\mathrm{SSIM} = \mathrm{Mean}\left[\frac{((2\times(d3))+c1)\times((2\times(\sigma_{12}))+c2)}{(a3+b3+c1)\times(\sigma_1+\sigma_2+c2)}\right] \qquad \ldots (5)$$

Where $a3, b3$ is the elementwise multiplication of matrix format of cover image and reconstructed image itself, respectively. d3 is the element wise multiplication of both. σ_1, σ_2 and σ_{12} is the difference between the matrix that represent the filtered image and the element wise multiplication of the corresponding image for cover image, reconstructed image and the combination of both. The rotational symmetric Gaussian low pass filter of size 11 with standard deviation of 1.5 is used. The value of c1 and c2 is selected as 6.5 and 58.52.

The figure 6 represents the increment in the PSNR value as the size gets increased. So the preferable size is 1024×1024. The embedding capacity is normalized to 7000bits. The simulation results (fig.7) show that the PSNR value is around 72.9dB where the embedding capacity varies from 10 bits to 7000 bits. It justifies the imperceptibility of the reconstructed image. The SSSIM value is obtained as 1.000 shows that these design methodology is robust against various attack such as scaling, cropping, JPEG compression, etc...

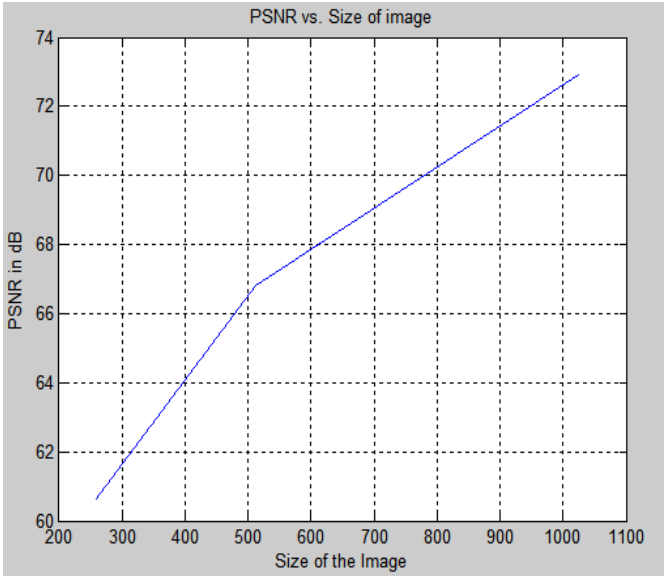


Fig.5. PSNR vs. size of image

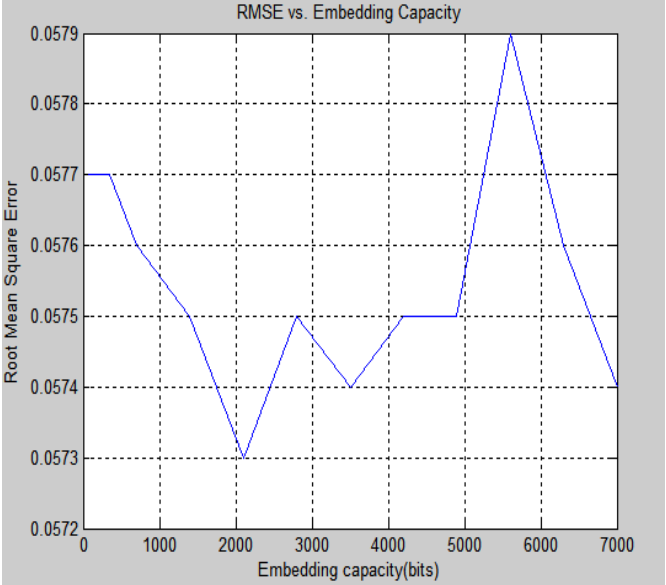


Fig.6. RMSE vs. embedding capacity

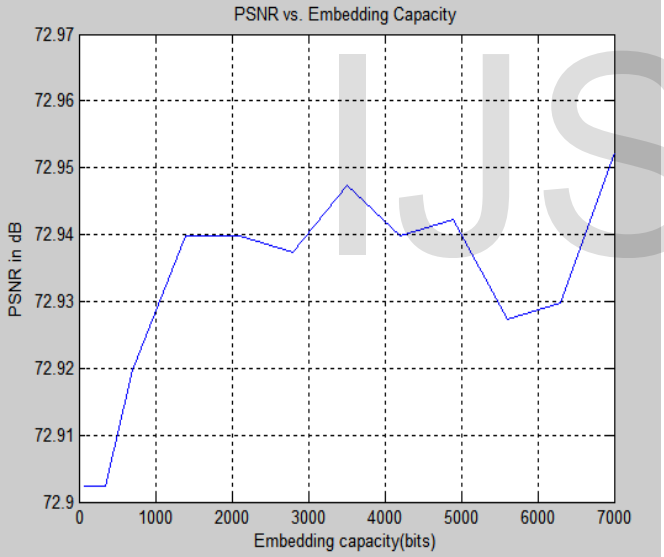


Fig.7. PSNR Vs Embedding Capacity

4. CONCLUSION

In this paper, we proposed A Novel Reversible Data Hiding Scheme (RDH) using Randomized Pixel Variation (RPV) which is on the basis of biological process of controlling the color of the cell by a pigment cell, named as melanocyte. The pixel pair mapping technique is utilized to select the pixel randomly to hide the data bit. The design methodology is enhanced to satisfy robustness, imperceptibility and high capacity simultaneously. Due to slight variation in the pixel values, the high image quality is preserved. The performance is analyzed using Peak Signal to Noise Ratio (PSNR) calculations and Structural Similarity (SSIM) index for watermark imperceptibility and robustness, respectively. The performance parameters are estimated as follows: Peak Signal to Noise Ratio (PSNR) as 72.95dB, Structural Similarity (SSIM) as 1, Root Mean Square Error (RMSE) as 0.05, information Rate as 1/150 bits/pixel and Computation Complexity as 1.511x10-3sec.

FUTURE WORK

Although the results obtained from this work are efficient enough, there are areas that can be improved to raise the overall accuracy or enhance the system. Even though this work focus on watermarking grayscale images, extensions into color images and video frames are possible because they all have similar data representation. However, the effects on the visual quality and watermark robustness need further investigation. The computation of this developed algorithm made simple to enhance this to the video which has 30 frames per second. The authentication is also to be enhanced by adding additional key to scramble the message and the hacking of the data is further framed to tough by finding the frame where the actual data is present.

REFERENCES

[1] Chih-Chin Lai, and Cheng-Chih Tsai (2010) "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 11, pp. 3060-3063.

[2] Chuntao Wang, Jiangqun Ni, and Jiwu Huang (2012) "An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 3, pp. 853-867.

[3] Dimitrios Simitopoulos, Dimitrios E. Koutsonanos, and Michael Gerassimos Strintzis (2003) "Robust Image Watermarking Based on Generalized Radon Transformations", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 8, pp. 732-745.

[4] Dong Zheng, Sha Wang, and Jiying Zhao (2009) "RST Invariant Image Watermarking Algorithm", IEEE Transactions On Image Processing, Vol. 18, No. 5, pp. 1055-1068.

[5] Ehsan Nezhadarya, Z. Jane Wang, and Rabab Kreidieh Ward (2011) "Robust Image Watermarking Based on Multiscale Gradient Direction Quantization", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 4, pp. 1200-1213.

[6] Gouenou Coatrieux, Wei Pan, Nora Cuppens-Boulahia, Frederic Cuppens, and Christian Roux (2013) "Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, pp. 111-120.

[7] Jen Sheng Tsai, Win-Bin Huang, and Yau-Hwang Kuo (2011) "On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking", IEEE Transactions On Image Processing, Vol. 20, No. 3, pp. 735-743.

[8] Jiantao Zhou, and Oscar C. Au (2012) "Determining the Capacity Parameter in PEE Based Reversible watermarking", IEEE Signal

Processing Letters, Vol. 19, No. 5, pp. 287-290.

[9] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong (2010) "Reversible Image Watermarking Using Interpolation Technique", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, pp. 187-193.

[10] Mehmet Utku Celik, Gaurav Sharma, and Murat Tekalp. A (2006) "Lossless Watermarking for Image Authentication: A New Framework and an Implementation", IEEE Transactions On Image Processing, Vol. 15, No. 4, pp. 1042-1049.

[11] Ming Chen, Zhenyong Chen, Xiao Zeng, and Zhang Xiong (2010) "Model Order Selection in Reversible Image Watermarking", IEEE Journal Of Selected Topics In Signal Processing, Vol. 4, No. 3, pp. 592-604.

[12] Mohammad Ali Akhaee, Sayed Mohammad Ebrahim Sahraeian, and Craig Jin (2011) "Blind Image Watermarking Using a Sample Projection Approach", IEEE Transactions On Information Forensics And Security, Vol. 6, No. 3, pp. 883-893.

[13] Shan He, Darko Kirovski, and Min Wu (2009) "High Fidelity Data Embedding for Image Annotation", IEEE Transactions On Image Processing, Vol. 18, No. 2, pp. 429-435.

[14] Xiaolong Li, Bin Yang, and Tieyong Zeng (2011) "Efficient Reversible Watermarking Based on Adaptive Prediction Error Expansion and Pixel Selection", IEEE Transactions On Image Processing, Vol. 20, No. 12, pp. 3524-3533.

[15] Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng (2011) "Watermarking With Flexible Self Recovery Quality Based on Compressive Sensing and Compositive Reconstruction", IEEE Transactions On Information Forensics And Security, Vol. 6, No. 4, pp.1223-1232.

[16] Xuan. G, Yao. Q, Yang.Q. C, Gao. J, Chai. P, Shi. Y and Ni. Z (2007) "Lossless data hiding using histogram shifting method based on integer wavelets", Proc. of 5th International Workshop on Digital Watermarking, Korea, Vol. 42, No. 83, pp. 323-332.

[17] Yang. B, Schmucker. M, Funk. W, Busch. C, and Sun. S (2004) "Integer DCT-based reversible watermarking for images using companding technique", Proc. of SPIE, Security and Watermarking of Multimedia Content, Electronic Imaging, San Jose, California, USA, Vol. 53, No. 6, pp. 405-415.