ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

International Journal of Development Research
Vol. 5, Issue, 10, pp. 5903-5908, October, 2015

Full Length Review Article

SECURE WATERMARKING TECHNIQUES FOR IMAGE AUTHENTICATION USING SVD

*Gagandeep Kaur and Baljit Singh Khehra

Department of CSE/IT, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, 140407, Punjab, India

ARTICLE INFO

Article History:
Received 11th July, 2015
Received in revised form
19th August, 2015
Accepted 06th September, 2015
Published online 31st October, 2015

Key Words:
Watermarking, Tenure confirmation,
Discrete Wavelet Transform,
Discrete Cosine Transform,
Singular Value Decomposition.

ABSTRACT

Digital watermarking is a practice that involves implanting furtive statistics into a host image and extorted out afterward for tenure confirmation. Execution plus concert examination of three diverse methods based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition are carried out. To verify efficiency of all these schemes for invisibility plus durability, various constraints are taken into consideration.

INTRODUCTION

During the earlier period of about ten to fifteen years, the digital world has achieved an extraordinary development. Conventional security methods, for instance, Steganography have been lifted up to look after ownership privileges for multimedia data. Along with the universal use of cyberspace plus different network topologies, countless digital multimedia statistics are accessible at present. These statistics can be entirely copied, personalized and broaden quickly without anybody even be aware of it. With an appropriate development in the field of computing system, these security procedures have considered to be outdated, since they are simpler to decrypt. Hence the security mechanisms presented by encryption no longer exist. Consequently, digital watermarking, the sculpture of hiding information in a dynamic and an indistinguishable way, has been considered as an equivalent technology. The enlarged cyberspace tradition has turned a technique with an intention to defend the patent of available medium into an essence. The effortless circulation of such credentials across the internet may possibly disobey security laws beside illegal editions or copies and make trustworthiness debatable. Digital watermarking is a resolution to all such problems.

Digital watermarking is a method to grant genuineness by suppressing a data into an image or audio or document. Digital watermarking has a spare necessity of durability in contrast to Steganography techniques beside probable assails. It must be distinguished that watermarking is not projected for shielding the content of a text or a message, therefore is singular from cryptography. In this examination we focus on the durableness of the digital watermarking algorithms in the transform domain beside ordinary assaults.

The image within which the secret data is infixed is described to be a host or a cover image and watermark is usually an additive noise indication there in the host signal. The watermark expansion desires to be bendable headed for possible infringements, preserving the statistics of the watermark comprehensible so that it could be acknowledged on the moment of drawing it out. Attributes such as durability along with reliability are fundamentals of a watermarking system. Though, the dimensions of the set in information have to be measured while the data turns out to be less durable as its dimensions increases. Hence compositions of these attributes have to be measured with awareness.

Depending on sphere tattered for watermark entrenching procedure the watermarking techniques are categorized into two categories:

- Spatial Domain Watermarking
- Frequency Domain Watermarking

***Corresponding author: Gagandeep Kaur,**
Department of CSE/IT, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, 140407, Punjab, India.

We have used DWT (Discrete Wavelet Transform) and DCT (Discrete Cosine Transform) for watermarking. The review of the watermarking techniques has been discussed in section II. The section III is proposed work which is followed by result analysis and experiment study. The paper is concluded in the last section.

Sharma Preeti and Jain Tapan (Preeti and Tapan Sukumar, 2014), presented a hybrid watermarking scheme using SVD and DWT, in which they fixed a watermark in remarkable positions of the red constituents of the DWT sub-bands of the coated image and then after pooled with the other two green and blue constituents to defer the marked image. Practical outcomes are prepared which illustrate the enhanced undetectability and durability under several interventions and maintain copyrights. Saini Hemraj (Hemraj Saini, 2014) projected a proficient method for digital watermarking by using DWT-SVD and BPNN. N. Mohammed *et al.* (Mohammed, 2014) tried acquiring improved NCC values that is used to improve the durability by introducing two bits of watermark image into each pixel of the host image on the present DISB system and the method is comparatively more precise than that of LSB.

Divecha Nidhi and Dr. N. N. Jani (Nidhi Divecha, 2013), projected a scheme that mingles the benefits of three dissimilar systems which are DCT, DWT and SVD. Kakkirala R. Krishna and Chalamala R. Srinivasa (Krishna Kakkirala, 2014) projected a block based blind image watermarking using SVD, DWT and Torus automorphism and is verified against several attacks. Singh Ranjeet Kumar *et al.* (2013) established a watermarking algorithm in which inserted mark was invisible by nature and based on the pixel block intensity values. Block intensity is attuned in a way that, it conceals the actual watermark image. Lastly with an IDCT function, marked image is transformed into the actual watermark image. Hun Fung Charles Way *et al.* (Charles Way Hun Fung, 2011) have evaluated various up to date contrivances and anticipated taxonomy based on their built-in characteristics, inserting techniques plus exposure types and obtained a fundamental four steps sculpt for the watermarking. Singh Shantikumar *et al* (2008) have examined the major Y. Singh Shantikumar *et al.* (2008) have examined the major practices in continuation for watermarking that are engaged in copyright protection. Jing-pei WANG *et al.* (2009) accessed a Media-Hash based digital watermarking scheme based on SVD.

The protocol attacks in SVD based scheme are gripped and handled successfully by taking up Media-Hash. Kekre *et al.* (2010) examined that the utilization of DCT-wavelet significantly picks up the realization of watermarking in contrast with of Haar wavelet transform in both the characteristics which are undetectability and durability. Choice of suitable value of scaling factor matters a lot in the proposed scheme. Kumar Sivadanam Bharath and Dr. Ramashri Tirumala (2011) offered and SWT-SVD combined full band watermarking method. The excellence of extorted watermark demonstrates that the projected algorithm is strong and the quality of cover image is not compromised. S. Mathapati Renuka and Pujari Jagadeesh (2012) analyzed that Digital Watermarking is a promising method over conventional encryption for digital rights management (DRM). Existing schemes for Digital Video Watermarking are conservatory so absolutely possibility of further modernization is there. Gupta Vinita and Mr. Barve Atul (2014) revealed the variety of watermarking techniques and applications of watermarking and likewise talked about a significant technology that is said to be QR code.

Chakraborty Sayan and Maji Prasenjit (2014) offered a scheme in which one can implant 10 bits of watermark in every solo block of an image. Thus in a 200 x 200 image one can insert 100000 bits of watermark. Hence, the payload or watermark size in this algorithm is tremendously elevated. Xiangui Kang *et al.* (2003) anticipated DWT-DFT merged watermarking method that is vigorous to affine transforms and JPEG compression simultaneously having higher PSNR and robustness. Moreover, a training cycle is entrenched in DWT domain to attain organization. An asset of DWT named as Dyadic is utilized to decrease DWT implementations radically so as to reduce the computational intricacies. Er. Aggarwal Deepak *et al.* (2010) anticipated a non-blind watermarking scheme which utilizes watermark nesting on level-1 DWT disintegration.

Chaturvedi Navnidhi and Dr. S.J. Basha (2012) evaluated DWT and DWT-DCT techniques on the basis of PSNR assessments having value 58.39 dB for DWT-DCT scheme and 51.466 dB for DWT respectively and after winding up the outcomes, concluded that DWT-DCT scheme is the paramount scheme for level one watermark insertion. Priya N. R. Nantha and Stuwart S. Lenty (2010) offered a superior supervision to adaptively amend the watermark set in potential using Noise Visibility Function (NVF). For the time being, the image stabilization and scale invariant feature (SIFT) extractions are applied to accomplish the rotation, scaling, and translation (RST) invariance. The spread spectrum and linear correlation are used for watermark insertion and recognition. Bas Patrick and Furon Teddy (Patrick Bas and Teddy Furon, 2012) planned a fresh evaluation entitled as an efficient key length to exemplify watermarking protection. They concluded that for an invariable error rate against the AWGN channel, the key length rises with respect to the length of the host and reduces with respect to the deformations.

N. Kaladharan (Kaladharan, 2014) reviewed that encryption and decryption algorithm is purposeful to meet the expense of privacy and security in communication of the picture based information as well as in storage. Dr. Jaleel J. Abdul and Thomas Jisha Mary (2013) worked with a goal to encode and decode with Blowfish algorithm that incorporates creation of gray scale images of different formats. The outcomes demonstrate that the encoded image supplies not any statistics regarding the actual data but the decoded data is nearly a carbon copy of an entered data. Mr. M. Falesh *et al.* (2014) suggested that dissimilar formats of images encompass diverse ways of hiding secret posts thus contain specific sturdy and fragile spots correspondingly, where some methods are short in consignment ability, whilst a few are deficient in durableness. So any algorithm has to be chosen with awareness and that can meet up the main requirements of the work. Kumar Arvind and Km. Pooja (2010) projected and defined certain frequent utilization of Steganography practices like thrashing or pasting information on the system as in infringement, peer-to-peer confidential interactions, deployment of furtive interactions on the internet, implanting curative audio or image information as in deterioration and might take place because of a deprived association between networks.

Proposed Work

As in today's era nothing is safe online and no matters in which form the data is. So, to make the data more secure which is communicated over the network different methods are taken into deliberation. The ambition of this study is centered on accomplishing digital watermarking utilizing three varied practices named as DCT, DWT and SVD in MATLAB by means of image processing toolbox. The projected approach appears to be competent as certain significant security trials are applied to encode the watermarked data at the time of transmission. Different images are taken into reflection and in each algorithm any two images are utilized. One out of which acts as a host image and other as a watermark which is supposed to convey messages secretly.

Further, the mixture of these two images forms a watermarked image. This is done by applying different SVD oriented transformation on cover as well as the watermark image. In addition, to make it more secure certain security parameters are applied during encoding of the watermarked data that can only be decoded with specific privileges. Then the process of de-watermarking is carried out in order to recover the original data. To verify efficiency of the exercised methods for invisibility plus durability, constraints like compression ratio (CR), mean square error (MSE), signal to noise ratio (SNR), and peak signal to noise ratio (PSNR) are considered.

A. SVD based DCT

Algorithm I

# Watermark Embedding

a) Input host image of size M*N.
b) Apply discrete cosine transform (DCT) on the input image.
c) Apply singular value decomposition (SVD) on the input image.
d) Input watermark image of size M*N.
e) Apply DCT on watermark image.
f) Apply SVD on DCT watermarked image.
g) To update 's' component for insertion do:

Snew = 'S' component of original image + α * SVD component of original image

h) Get the watermarked image by applying the following equation:
i)

Imagenew = 'U' component of original image * Snew * 'V' component of original image

j) Apply inverse DCT on the Imagenew.

# Encoding and Decoding

a) Input image for encoding.
b) Generate and insert a security key based on bit-XOR method.
c) Production will be an encoded image.
d) Take encoded image as an input image.
e) Insert a security key based on bit-OR method.
f) Production will be a decoded image.

# Watermark Extraction

a) Input decoded image.
b) Apply DCT on decoded image.
c) Apply SVD on DCT decoded image.
d) To update 'S' component for extraction do:

Snew = ('S' component of original image – 'S' component of) / α

e) Get the watermarked image by applying the following equation:

Imagenew = 'U' component of watermark image * Snew * 'V' component of watermark image

f) Apply inverse DCT on the Imagenew.
g) Production will be an extracted watermark image.

B. SVD based DWT

Algorithm II

# Watermark Embedding

a) Input host image of size M*N.
b) Apply discrete wavelet transform 1-(DWT) on the input image.
c) Apply discrete wavelet transform 2-(DWT) on the input image.
d) Apply singular value decomposition (SVD) on HH bands of the input image.
e) Input watermark image of size M*N.
f) Apply DWT on watermark image.
g) Apply SVD on DCT watermarked image.
h) To update 's' component for insertion do:

Snew = 'S' component of original image + α * 'S' component of (g)

i) Get the watermarked image by applying the following equation:

Imagenew = 'U' component of original host image * Snew * 'V' component of original host image

j) Apply inverse DWT on the Imagenew.
k) Output will be a watermarked image.

# Encoding and Decoding

a) Input image for encoding.
b) Generate and insert a security key based on bit-XOR method.
c) Production will be an encoded image.
d) Take encoded image as an input image.
e) Insert a security key based on bit-OR method.
f) Production will be a decoded image.

# Watermark Extraction

a) Input decoded image.
b) Apply DWT on decoded image.
c) Apply SVD on HH bands of the watermarked image.
d) To update 'S' component for extraction do:

Snew = ('S' component of original image – 'S' component of watermarked image) / α

e) Get the watermarked image by applying the following equation:

Imagenew = 'U' component of watermark image * Snew * 'V' component of watermark image

f) Apply inverse DWT on the Imagenew.

g) Production will be an extracted watermark image.

C. Hybrid SVD based DCT and DWT

Algorithm III

# Watermark Embedding

a) Input image of size M*N.

b) Apply discrete cosine transform 1-(DWT) on the input image.

c) Apply discrete cosine transform 2-(DWT) on the input image.

d) Apply discrete cosine transform (DCT) on the image (c).

e) Apply singular value decomposition (SVD) on the image (d).

f) Input watermark image of size M*N.

g) Apply DWT on watermark image.

h) Apply DCT on the image (g).

i) Apply SVD on DCT watermarked image (h).

j) To update 's' component for insertion do:

Snew = 'S' component of original image (e) * α * 'S' component of (i)

k) Get the watermarked image by applying the following equation:

Imagenew = 'U' component of original image
**** Snew * 'V' component of original image***

l) Apply inverse DCT on the Imagenew.

m) Apply inverse DWT on image (l).

n) Production will be a watermarked image

# Encoding and Decoding

a) Input (n) image for encoding.

b) Generate and insert a security key based on bit-XOR method.

c) Production will be an encoded image.

d) Take encoded image (c) as an input image.

e) Insert a security key based on bit-OR method.

f) Production will be a decoded image.

# Watermark Extraction

a) Input decoded image (c).

b) Apply DWT on decoded image.

c) Apply DWT on LL bands of image (b).

d) Apply DCT on HH bands of image (b).

e) Apply SVD on image (d).

f) To update 'S' component for extraction do:

Snew = ('S' component of original image – 'S' component of watermarked image) / α

g) Get the watermarked image by applying the following equation:

Imagenew = 'U' component of watermark image * Snew * 'V' component of watermark image.

h) pply inverse DCT on the Imagenew.

i) Apply inverse DWT on the Imagenew.

j) Apply inverse DWT on the Imagenew.

k) Production will be an extracted watermark image.

RESULTS

We have taken some standard images in different formats. Then all the three algorithms as mentioned above have been applied on the images. After performing these experiments, we have calculated the PSNR (Peak Signal Noise Ratio) value for all the images for all the three algorithms. This experiment shows that which algorithm gives better results.

The images used for experiment study are as follows:

Image 1

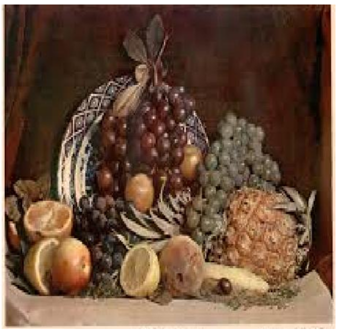

Image 2

Image 4

Image 5

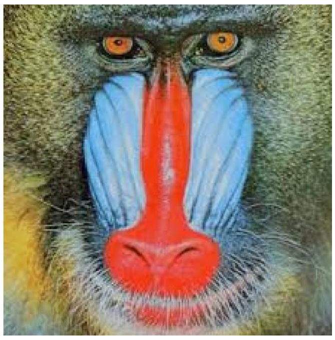

Image 6

Table 1. PSNR of Images used as Watermark Image

Images	Algorithm I	Algorithm II	Algorithm III
Image 1	5.71	6.07	6.64
Image 2	7.24	8.92	8.15
Image 3	7.13	8.70	9.29
Image 4	7.24	7.50	7.96
Image 5	6.56	7.74	8.35
Image 6	7.90	9.95	9.93

Table 2. SNR of Images used as Watermark Image

Images	Algorithm I	Algorithm II	Algorithm III
Image 1	2.46	2.82	3.40
Image 2	1.12	2.80	2.03
Image 3	1.34	1.81	2.40
Image 4	3.19	3.44	3.91
Image 5	1.89	3.67	1.36
Image 6	1.97	4.03	4.06

From the above tables, we analyze that the hybrid technique gives best quality of image. The formula for PSNR is as follows:

PSNR = 10 log10 (R2 / MSE)

Where,

MSE = sum ((I1 (m, n) – I2 (m, n)) 2) / m*n

R is the maximum fluctuation of pixels and m, n are the row and column matrix of the images.

From the formula, we can easily see the relation between MSE, PSNR and image quality. The MSE is mean squared error which have to be low for better quality. The MSE is in reciprocal of PSNR that is why if MSE will be low the PSNR will be high. For the same reason, from the above table I the PSNR of the extracted images are high for algorithm III as comparison to other algorithms. In algorithm III the reconstruction of image will be easy. The data of the table I has been graphically represented as follows:

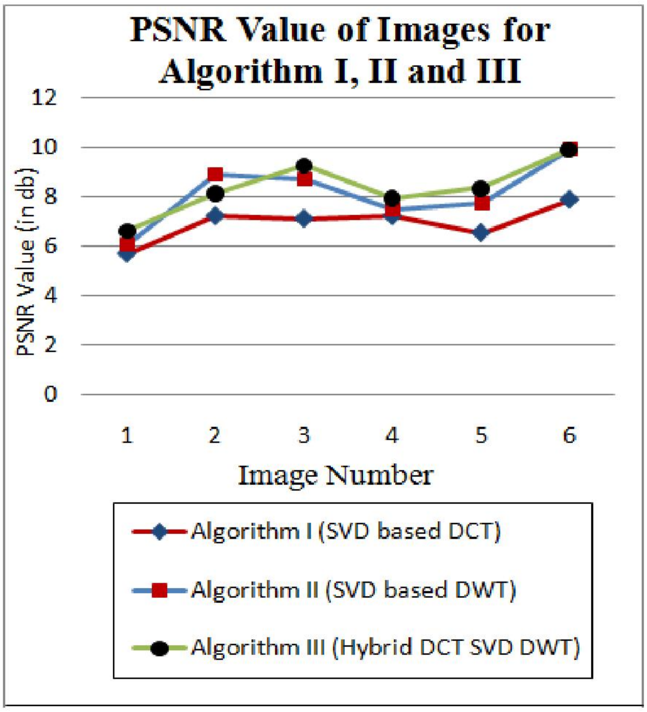

Figure 1. PSNR Value comparison of Algorithm I, II and I

After conducting experiments with all the three algorithms, we take some experiments on images after the attacks of different noises.

The following tables collect the data regarding the affects of different noise attacks on the quality of images and PSNR value variation.

Table 3. PSNR value after Salt and Pepper Noise Attack

Salt and Pepper Noise						
Scale Factor	0.01	0.02	0.04	0.06	0.08	0.09
Image 1	24.03	20.94	17.99	16.22	15.00	14.52
Image 2	24.66	21.38	18.56	16.85	15.52	15.00
Image 3	25.85	21.99	19.03	17.18	16.01	15.51
Image 4	24.75	21.69	18.70	16.84	15.59	15.16
Image 5	24.71	21.63	18.68	16.93	15.71	15.10
Image 6	25.52	22.27	19.40	17.62	16.24	15.77

Table 4. PSNR value after Speckle Noise Attack

Speckle Noise						
Scale Factor	0.01	0.02	0.04	0.06	0.08	0.09
Image 1	25.39	22.44	19.46	17.72	16.52	15.98
Image 2	26.60	23.76	20.98	19.35	18.21	17.74
Image 3	26.99	24.05	21.16	19.47	18.30	17.82
Image 4	24.54	21.72	18.97	17.37	16.28	15.84
Image 5	28.49	25.56	22.66	20.97	19.79	19.31
Image 6	25.97	23.05	20.16	18.48	17.32	16.81

Table 5. PSNR value after Gaussian Noise Attack

Gaussian Noise						
Scale Factor	0.01	0.02	0.04	0.06	0.08	0.09
Image 1	21.32	21.27	21.05	20.56	19.93	19.54
Image 2	20.49	20.36	19.83	19.14	18.34	17.94
Image 3	20.21	20.06	19.53	18.84	18.03	17.57
Image 4	20.52	20.44	20.03	19.41	18.69	18.29
Image 5	20.36	20.19	19.65	18.94	18.13	17.66
Image 6	20.08	19.97	19.50	18.81	18.03	17.62

Conclusion

After implementing the three methods of blind image watermarking which are SVD based DCT, SVD based DWT and hybrid SVD based DCT and DWT, one can easily finish if off by illustrating the best results provided by the last hybrid technique. As it is clear from the experimental outcomes that the first algorithm presents the worst results as compared to the other two techniques and the second algorithm offers the improved results than that of the DCT and the third hybrid algorithm proposes the superior consequences.

Future Scope

A tailored SVD based watermarking to augment the fallouts to an even more extent plus utilization of implanting ++ to boost the sanctuary even more shall soon be recommend. Moreover, several more assails will be absorbed to weigh up the concert of the anticipated algorithms.

REFERENCES

Arvind Kumar, Km. Pooja, 2010. “Steganography- A Data Hiding Technique”, *International Journal of Computer Applications*, pp. 19-23.

Charles Way Hun Fung, Antˆonio Gortan and Walter Godoy Junior, 2011. “A Review Study on Image Digital Watermarking”, The Tenth International Conference on Networks, pp. 24-28.

Dr. J. Abdul Jaleel, Jisha Mary Thomas, 2013. “Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm”, *International Journal of Engineering and Innovative Technology*, pp. 196-201.

Er.Deepak Aggarwal, Er.Sandeep Kaur and Er.Anantdeep, 2010. “An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality”, *Journal of Computing*, pp. 105-109.

Hemraj Saini, S. 2014. “Efficient hybrid Watermarking Approach by Using SVD, DWT, and Back Propagation Neural Network”, *IEEE International Advance Computing Conference,* pp. 985-990.

Kaladharan N, 2014. “Unique Key Using Encryption and Decryption of Image”, *International Journal of Advanced Research in Computer and Communication Engineering*, pp. 8102-8104.

Kekre, H. B., Tanuja Sarode and Shachi Natu, 2013. “Hybrid Watermarking Of Color Images Using DCT-WAVELET, DCT and SVD,” *International Journal of Advances in Engineering and Technology*, pp. 769-779.

Krishna Kakkirala, R. and Srinivasa Chalamala, R. 2014. “Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform”, 10th *IEEE International Colloquium on Signal Processing and its Applications,* pp. 58-61.

Mohammed, N., Azman Yasin and Akram M. Zeki, 2014. “Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB) Ghassan”, 6th *IEEE International Conference on CSIT*, pp. 18-22.

Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, 2014. “Comparison of different techniques for Steganography in images”, *International Journal of Application or Innovation in Engineering and Management*, pp. 171- 176.

Nantha Priya, N.R., Lenty Stuwart, S. 2010. “Robust Feature Based Image Watermarking Process”, *International Journal of Computer Applications*, pp. 13-16.

Navnidhi Chaturvedi, Dr. S.J. Basha, 2012. “Comparison of Digital Image watermarking Methods DWT and DWT-DCT on the Basis of PSNR”, *International Journal of Innovative Research in Science, Engineering and Technology*, pp. 147-153.

Nidhi Divecha, D. and Dr. Jani, N. N. 2013. “Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images”, International Conference on Intelligent Systems and Signal Processing, pp. 204-208.

Patrick Bas and Teddy Furon, 2012. “The Effective Key Length of Watermarking Schemes”, *IEEE Transactions on Information Forensics and Security*, pp. 1-22.

Preeti, S. and Tapan Sukumar, J. 2014. "Robust Digital Watermarking for Colored mages using SVD and DWT Technique", IEEE *International Advance Computing Conference,* pp. 1024-1027.

Ranjeet Kumar Singh, Shikha Gupta, Deepak Gupta, 2013. “A Secure Authentication Technique using Edge Detection in Watermarking”, *International Journal of Computer Applications*, pp. 41-44.

Renuka, S. Mathapati, Jagadeesh, Pujari, 2012. “Digital Video Watermarking”, *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. 1-8.

Sayan Chakraborty and Prasenjit Maji, 2014. “Reversible Color Image Watermarking using Trigonometric Functions”, IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies, pp. 105-110.

Shantikumar Singh, Y. Pushpa Devi, B. and Kh. Manglem Singh, 2013. “A Review of Different Techniques on Digital Image Watermarking Scheme”, *International Journal of Engineering Research*, pp. 193-199.

Sivadanam Bharath Kumar, Dr. Tirumala Ramashri, 2011. “Robust SWT SVD Based Digital Image Watermarking Technique” *International Journal of Computer Science information and Engineering Technologies*, pp. 1-4.

Vinita Gupta and Mr. Atul Barve, 2014. “A Review on Image Watermarking and Its Techniques”, *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. 92-97.

WANG Jing-pei, SUN Shui-fa, JIANG Ming, XIE Dan-gui and LEI Bang-jun, 2009. “Anti-protocol attacks digital watermarking Based on Media-Hash and SVD”, 5th IEEE *International Conference on Information Assurance and Security*, pp. 364-367.

Xiangui Kang, Jiwu Huang, Senior Member IEEE, Yun Q. Shi, Senior Member, IEEE, and Yan Lin, 2003. “A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression”, *IEEE Transactions on Circuits and Systems for Videos Technology*, pp. 776-786.

****