

A Hybrid Novel Approach of Video Watermarking

Manoj Kumar¹, Sangeet Sriastava² and Arnold Hensman³

¹*JIMS Engineering Management Technical Campus, Greater Noid*

²*North Cap University, Gurgaon*

³*School of Informatics and Engineering, ITB, Dublin (Ireland)*

¹*wss.manojkumar@gmail.com, ²sangeet.srivastava@ncuindia.org,*

³*arnold.hensman@itb.ie*

Abstract

The rapid evaluation of image manipulation and tampering has evoked the need for protecting digital data. Therefore a copyright protection method is used to protect the user information known as watermarking. Watermarking is the major image processing technique used to authenticate digital data. In this paper a hybrid approach is proposed to protect the digital data and also authenticates the user information. The proposed approach is an improvement over traditional video watermarking approaches. It uses fractions from the watermarked image to embed into the unique frames of the original video. The whole approach is divided into three steps which are described in the next sections of this paper. To check the resilience and robustness of this approach, various attacks are implemented over the watermarked video. After attacks, watermark image is extracted from the watermarked video to check the robustness of this approach. The quality of the recovered watermarked image is analysed using bit error rate. Experimental results show that this approach is very robust compared to other approaches.

Keywords: *Invisible Video Watermarking, Visual Cryptography, Copyright Protection, Identity Authentication*

1. Introduction

Digital watermarking is a technique to authenticate digital data in the form of images, documents or videos. Watermarking provides copyright protection to the digital data by hiding some appropriate information. Watermarking itself is categorized into two broader types called visible and invisible watermarking [1]. The visible watermarking is placed in the background of the digital document to signify the owner or the authority name. Visible watermarks are easy to place because they just remove the pixel information from the position where the watermark is placed. Because of this, the invisible watermarking is suggested where a high level of authentication is required. Invisible watermarking is about to hide the authenticated information behind digital data without informing the type of data and its location. The main watermarking requirements are Robustness, Fidelity, Payload Capacity and reliability [2]. The approach implemented in this paper follow all these requirements. Video watermarking techniques are used in various applications such as Copyright Protection, Broadcast Monitoring, Data Authentication, Owner Identification, Fingerprinting and Security [3].

Video watermarking techniques are classified into two categories: Spatial Domain and Frequency Domain. Spatial domain techniques embed watermarks in the pixels of video frames directly while the later approach modifies the transform coefficients of video frames and embeds the data into it. It makes watermarking a robust approach. Frequency domain techniques are also imperceptible compared to spatial domain techniques [4]. Different techniques used for video watermarking are discussed in Section 2. The

purposed model uses a wavelet transformation technique to identify unique frames from a video. This approach encrypts the watermark symbol first and then embeds k sub pixels from the watermarked image on the video frames using histogram- based reversible data hiding. The scheme provides high degree of authentication, video quality and robustness. This paper is organized into five Sections: Section 2 presents literature work in this field. Section 3 show proposed scheme and Section 4 and 5 show results and conclusions.

2. Literature Work

In this section existing watermarking techniques are discussed. A good video watermarking algorithm must be robust against video compression, frame dropping, frame swapping, geometric attacks, frame rate conversion, frame cropping, collusion attacks, noise, filtering, lighting change, histogram equalization, *etc.*, [24] and [5]. Watermarking techniques are divided into three types, spatial domain, frequency and MPEG coding structure as shown in Figure 1.

a. Spatial Domain Techniques

These techniques are easy to implement. Using these techniques watermarks are embedded into pixels and no transformations are applied during the embedding process but before embedding data is transformed to frequency domain [6]. Spatial domain watermarking techniques are simple with low time complexity. Redundant part of the carrier signal is used for embedding digital data [1] and [24].

A.1. Correlation based Techniques

This is a simple method for adding watermark over an image. In this technique pseudorandom noise pattern is added in the luminance values of pixels [7]. Using this technique watermark is added to the original content by using Equation 1.

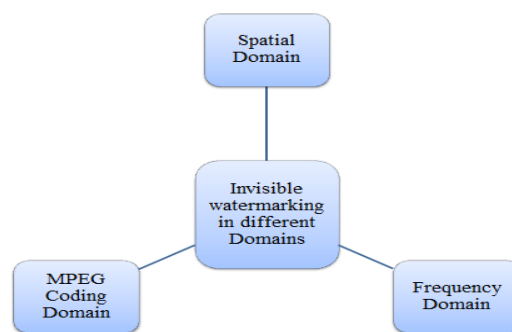


Figure 1. Classification of Invisible Digital Video Watermarking

In this equation, $I(x,y)$ is cover object while $W(x, y)$ pseudorandom noise pattern. Figure 2, shows the embedding procedure of this domain.

$$I_w(x, y) = I(x, y) + kW(x, y) \dots \dots \dots (1)$$

In this equation k is a gain factor while I_w is watermarked image. During the recovery process, correlation values between watermarked image and noise pattern is computed. This technique can be extended to multiple bit watermarking [7].

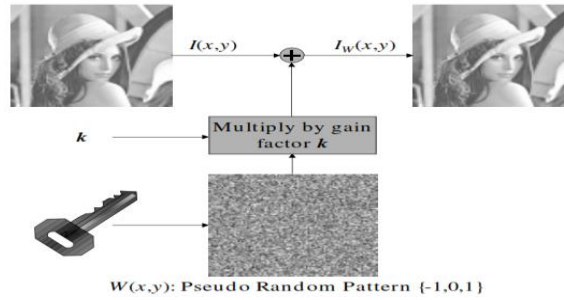


Figure 2. Watermarking in Spatial Domain

A.2. LSB Based Modifications

This is one of the simple method for watermarking where each pixel of gray image is divided into 8-bit planes. This technique possesses poor robustness and does not have visually appropriate information. More advanced techniques using this method are discussed in [8-9].

b. Frequency Domain Watermarking Techniques

Frequency domain techniques use DCT and DWT methods for data transformation. These methods are more powerful over correlation based watermarking but these methods require more computational power.

B.1. Discrete Cosine Transformation

DCT based techniques propose more correlation among pixels, in this frame is divided into different frequency bands respectively low, medium and high. Embedding data using middle band provides more robustness and security to the data [7]. The 2D watermark signal is divided into 8×8 DCT blocks and from these blocks frequency coefficients are modulated using Equation 2.

$$I_{w_{xy}} = I_{x,y}(u,v) + k \times W_{x,y}(u,v) \text{ if } u,v \in F_m \quad (2)$$

$$I_{x,y}(u,v) \text{ else}$$

T is the image and W represent watermark data. F_m denotes the frequency band with gain factor k and (u, v) are the DCT coefficients in 8×8 block [1].

B.2. Discrete Wavelet Transformation

This transformation divides an image into horizontal, diagonal and vertical components/ bands. This technique embed data in the DWT bands because doing this provide high resolution so that even a human eye cannot see the hidden information. DWT coefficients in these three bands can be modulated by using the Equation 3.

$$I_{w(u,v)} = I_{(u,v)} + k \times W_{(u,v)} \quad (3)$$

All the watermark data can be embedded over all the pixels contrary to DCT technique. DWT based techniques are more robust, stable and provides high imperceptibility [10].

B.3. Discrete Fourier Transformation

First discrete Fourier transformation is applied to original data and then the watermark is embedded in the modified frequency domain elements. iDFT (Inverse DFT) is applied

for recovery process. Kelker *et. al.*, [11] implemented JAWS (Just another Watermarking System) for broadcast monitoring applications. They used spatial domain which essentially compresses and decompresses the videos. They embed the same watermark into consecutive video frames using Gaussian and high pass filters. C.D Rawat [12] proposed a hybrid technique of DCT-DWT and Singular Value Decomposition (SVD). In this approach, they embedded a watermark in the image using DCT-SVD, DWT-SVD and DCT-DWT-SVD.

c. Watermarking Based on MPEG Coding

These type of watermarking scheme are used to provide integrated watermarking and compression to the data. Compression in MPEG-2 is achieved by taking forward and bi-directional motion prediction to remove temporal redundancy while the statistical method removes spatial redundancy. This technique is not vulnerable against re-compression and format conversion [13-24]. The basic principle of this technique is that it splits I-frames into 8×8 pixels which are later compressed by using the DCT quantization, zig-zag-scan, run level coding and entropy coding, as shown in Figure 3. P and B frames are motion compensated while residual prediction error signal frames are split into a block of 8×8 pixels. In the next step, the watermark block is transferred using DCT [1] and added as shown in Figure 3.

d. Histogram Based Watermarking

This approach of data hiding work on shifting phenomenon of bits. It first shift the bits and then embeds secret data in between neighbour bits of the original signal. Ni *et. al.*, [14] firstly proposed histogram based reversible data hiding. After embedding data using this scheme, authors recovered the image successfully without any distortion in the secret image. Authors in this extracted the peak points from the image histogram and then embedded data just by changing the grayscale pixel values.

The main feature of histogram based data hiding is that after embedding data, the original histogram peak disappears and shows a concave shape in the peaks known as “pair effect phenomenon”. Figure 4, shows that histogram peaks and its adjacent bin decrease after data embedding [1]. For loss less recovery these peaks and zero (Minimum) points are key parameters [15].

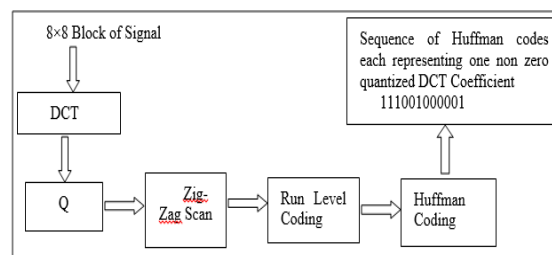


Figure 3. DCT Encoding on 8x8 Signal Block [13]

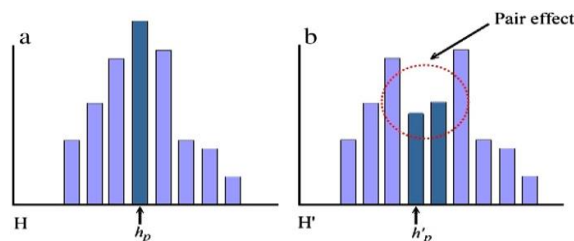


Figure 4. Pair Effect of a Histogram in (a) Cover-Image and (b) Stego-Image

e. Visual Cryptography Based Watermarking

This technique is based on encryption of data where data is encrypted using a key and without knowing the key reverse of this process becomes almost impossible. This technique is first introduced by Shamir & Naor in [16]. They divided the image into some shares then these shares are embedded into the original signal/data. Extraction from this technique is only possible if we can extract both the shares from the covered signal. Every pixel from the input image is divided into blocks of two parts where one contains the white and another contains black block [1]. Combining these blocks gives a binary image. According to Naor. M algorithm each pixel of the binary image is divided into 2×2 pixels as shown in Figure 5. As a result, we can get a $M \times N$ image into $2M \times 2N$ sharing images. More improvements using this technique can be studied from [17-19].

3. Proposed Watermarking Model

In this research model, an intelligent layered approach is suggested to perform the video watermarking. Instead of hiding the complete watermark image over the video, visual cryptography approach is proposed in this work [1]. This approach is capable of hiding high capacity information on the video frames. A histogram based reversible watermarking is used to perform the watermarking in video frames. Watermarking over the unique video frames will be performed sequentially after getting unique set $\{U\}$. The basic layered architecture is shown as in Figure 6. The layers and steps are interchangeable which are same by their meanings. Every layer includes different techniques.

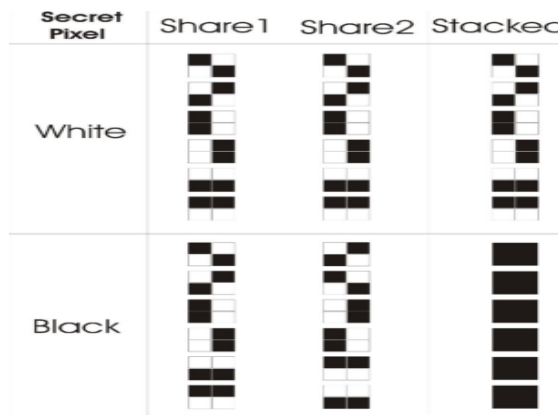


Figure 5. A 2x2 Visual Secret Scheme using 2x2 Pixels

Step 1:

In the first step, unique frames are extracted from the video $\{V\}$. Firstly, 2D wavelet decomposition is applied on the video frames and then a threshold value is used to obtain unique frames from decomposed frames. Based on the similarity matrix between the frames, unique frames $\{U\}$ were extracted from all the video frames $\{U_{in}\}$. 2D Wavelet Transform on each subsequent frame is used to create a set of Unique frames i.e. $\{U\}$. The aim of this step is to derive a factor that is affected by the luminance L_{xy} , contrast C_{xy} and edge structure similarity SIM_{xy} between the given input image(s) [1]. The computing equation to obtain these values are shown in Equation (4) (5) (8). The values of M_x , M_y , S_x and S_y are obtained. M denotes the mean value of the image in X and Y direction while S denotes the standard deviation of the Image in X and Y direction [1].

$$L_{xy} = \frac{(2 \times M_x \times M_y + Const1)}{(M_x \times M_x + M_y \times M_y + Const1)} \quad (4)$$

$$C_{xy} = \frac{(2 \times S_x \times S_y + Const2)}{(S_x \times S_x + S_y \times S_y + Const2)} \quad (5)$$

The Edge Structure Similarity between frames has been done using equations (6) and (7). To obtain the structural similarity we are using horizontal, vertical and diagonal wavelet coefficients of video frames (H, V, D respectively) [1].

$$E_{map_x} = \sqrt{(H1 \times H1 + V1 \times V1 + D1 \times D1)} \quad (6)$$

$$E_{map_y} = \sqrt{(H2 \times H2 + V2 \times V2 + D2 \times D2)} \quad (7)$$

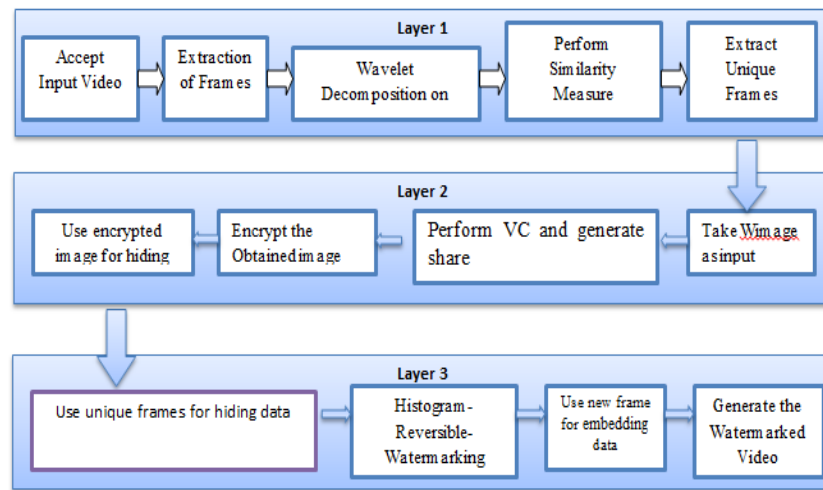


Figure 6. Layered Structure of the Proposed Model

The covariant standard deviation of these values are obtained. The SIM_{xy} is obtained using Equation 8.

$$SIM_{xy} = \frac{(Cov(2,1) + C3)}{S1_x \times S1_y + C3} \quad (8)$$

A threshold value is used to compare the uniqueness between video frames. The overall unique factor denoted by SIM (similarity) is obtained by using Equation 9:

$$SIM = [(L_{xy})(C_{xy})(SIM_{xy})] \quad (9)$$

Structure-based image similarity metrics were first proposed by Wang *et.al.*, in [20]. Based on a provided threshold the similarity value is analyzed to identify a unique frame from input video. From this process a set of unique frames $\{U\}$ from the video has been obtained [1]. These unique frames are further used for data hiding in step 2.

Step 2:

In this step, visual cryptography is performed. Using visual cryptography, share from the original image $\{I\}$ is generated and encryption of the image in the form of a share is used to generate the encrypted image $\{I'\}$. This procedure is used to obtain a 2D

encryption of the given input image I . In the pre-processing of this step calculation of the mean μ of the watermarked image frame $\{I\}$ of size $M \times N$ has been done.

- A seed value is used as a key k for the encryption and decryption process.
- The owner share size of $2M \times 2N$ from the watermarked image is generated which will further be used to embed into the unique frames of the video.
- Black and white shares are obtained based on the following rules as shown in Table 1.
- An image obtained from this algorithm is used as the encrypted image $\{I'\}$ which is further used for embedding in the video using step 3.

Step 3:

Histogram based shifting methods use a histogram of the image and modify grayscale pixel values to embed the data. Using this technique I' is embedded in all the unique frames of set $\{U\}$. In this algorithm an input frame $f(i)$ and the encrypted image from the previous step *i.e.*, $\{I'\}$ are provided. $f(i)$ is a grayscale image based on the histogram shifting approach.

Table 1. Visual Cryptography Share Generation Rule

Rule	Mean	BW	Block
1	$I(\text{Row, Col}) < \text{Mean}$	$\text{BW}(\text{Row, Col}) = 0$	
2	$I(\text{Row, Col}) < \text{Mean}$	$\text{BW}(\text{Row, Col}) = 1$	
3	$I(\text{Row, Col}) \geq \text{Mean}$	$\text{BW}(\text{Row, Col}) = 0$	
4	$I(\text{Row, Col}) \geq \text{Mean}$	$\text{BW}(\text{Row, Col}) = 1$	

Now scan the input image $f(i)$ in a sequential order and alter the intensity values by adding one based on the conditions mentioned-below [1]:

$$f(i)_{xy} = f(i)_{xy} + 1 \text{ if } Max_x \geq f(i)_{xy}$$

$$f(i)_{xy} = f(i)_{xy} + 1 \text{ if } Max_x < f(i)_{xy} \leq Min_x$$

In this condition Max_x and Min_x are the maximum intensity corresponding to Max count and minimum intensity corresponding to Min count of the image. In the next step scan the image again and embed the image $\{I'\}$ using the following conditions:

$$f'(i)_{xy} = f(i)_{xy} \text{ if } Max_x = f(i)_{xy} \text{ and } I'_{xy} = 0$$

$$f'(i)_{xy} = f(i)_{xy} + 1 \text{ if } Max_x = f(i)_{xy} \text{ and } I'_{xy} = 1$$

$$f'(i)_{xy} = f(i)_{xy} \text{ Otherwise}$$

By using above-mentioned equations we embedded the encrypted image I' into the video V and obtained watermarked video V' . $f'(i)$ is the pixel value of stego image $\{I'\}$. The max and min count are the key parameters for lossless recovery. This will be used to compare with the recovered algorithm output in the next step [1]. The factors like PSNR, MSE, and Similarity Ratio etc. will be calculated and discussed in later section.

Watermark Recovery Procedure

For all attacked frames of the video V' , the Reversal of the Histogram based Data Hiding approach is performed. It provides an input frame $f''(i)$ which we will be obtained after performing attacks. The input frame image i.e. $f''(i)$ is scanned in same sequential order and reverse the altered pixel intensity values based on the conditions mentioned below:

$$I?(i)_{xy} = 0 \text{ if } f''(i)_{xy} \leq \text{Min}_x = f?(i)_{xy}$$

$$I?(i)_{xy} = \text{Max}_x + 1 = f?(i)_{xy}$$

The image obtained will be a watermarked attacked image. Now, scan the image again and obtain the image $Irev(i)$ using the following conditions:

$$Irev(i)_{xy} = f(i)_{xy} \text{ if } f(i)_{xy} \leq \text{Max}_x \text{ and } f(i)_{xy} \geq \text{Min}_x$$

$$Irev(i)_{xy} = f(i)_{xy} - 1 \text{ if } \text{Max}_x < f(i)_{xy} \text{ and } f(i)_{xy} \leq \text{Min}_x$$

This will generate the final output reversible stego image. This model manipulates the fact that video is a combination of frames. When a small subset of the watermark pixels is applied to specifically chosen frames only, and then combine all frames to complete the video, the visible watermark will effectively be rendered invisible [1].

4. Experimental Results

After performing all the three steps, a watermarked video V' is obtained. In this section, various attacks are performed on the watermarked video V' to check the robustness of this technique. The intentional or unintentional attacks performed on the V' are Salt and pepper, Gaussian Noise, Unsharp, Median Filter, Crop, Rotate, Frame Averaging, Weiner Denoise, Frame Blending and Quantization [1].

A test case is a set of images and videos for this proposed work testing which go through this watermarking processes to determine the correctness of all the outcomes and their functioning. The test case is composed of five images and five videos of various sizes and specification. The performance is evaluated under different kind of attacks. Every video is tested with all the watermark images. Different formats of images are used, is one of the objective to prove the applicability of this watermarking model. Figure 7, shows the used watermarked image and videos for performing this experiment. In the first test case, first video is processed with all the five watermarked images and corresponding PSNR, MSE and BER are calculated. Histogram representation of different test cases are shown in Figure 8. Recovered images are analyzed using changes in the bits between the embedded binary image and recovered image after performing different attacks on the videos. Bit error rate is used to analyze the robustness. From all the test cases, average PSNR and Mean square error is obtained. The average PSNR is 33.6 and MSE of the watermarked video before the attack is 24.6 and after the attack it approaches to 26.2. There is slight change in the MSE values for all the test cases while PSNR decreases slightly. Overall this experiment gives satisfactory performance regarding the robustness and imperceptibility. The below-shown Graph 1 is a graphical representation between the obtained Attack vs. BER values [1]. The formulas used to calculate PSNR, MSE and BER in this paper are calculated by using following formulas. I_m is input image.

$$PSNR = 10 \log_{10} \left(\frac{(255)^2}{MSE} \right)$$

$$BER = (I_{in} + Noise) / I_{in}$$

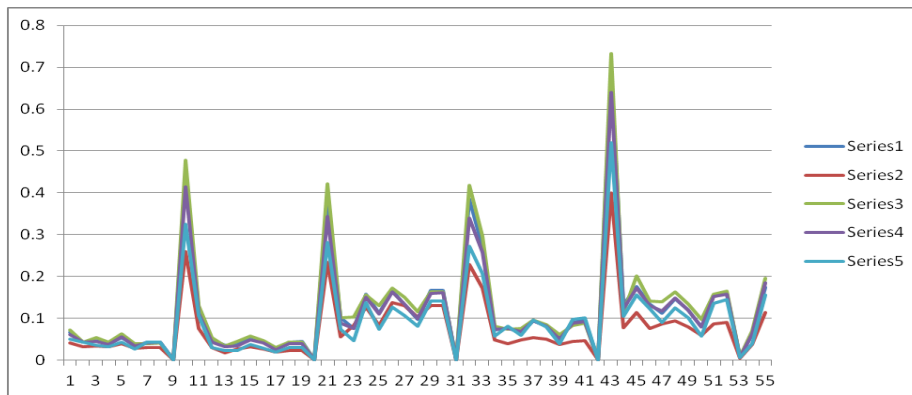
$$MSE = \frac{1}{xy} \sum_{i=1}^x \sum_{j=1}^y [A(i, j) - B(i, j)]^2$$

It represents five series of test cases. This graph represents curve of BER values for various attacks implemented. The graph shows that the random and Quantization attacks affect the videos to a maximum, thus causing various peaks to occur around each multiple of 11 *i.e.*, 11, 22, 33 *etc.*, as we have implemented 11 attacks in total. Quantization attack affects the video more compared to other attacks in this work. Table 2, shows the maximum and minimum bit error rate [1].

Table 2. Concluded Maximum and Minimum BER values

MAX	0.34	Quantization
MIN	0.0028	Frame Blending

This proposed technique compared to [21-23] and [6] techniques is more efficient and robust.



Graph 1: BER vs. Attack Values (for all Test Case Series)



Figure 7. Test Set for the Proposed Technique (Five Videos and Five Images)

5. Conclusion and Future Work

The obtained results from this hybrid watermarking model indicate that this technique provides robustness and fidelity to the watermarked video with moderate payload capacity. This technique provides better recovery of watermarked image after performing various attacks. This watermark model fulfils all the requirements suits to video watermarking as mentioned in Section I. This hybrid approach is unique and provides better results for watermarking. For further improvements, the watermarked video quality can be improved by adding more payload data and by optimizing quantization attack.

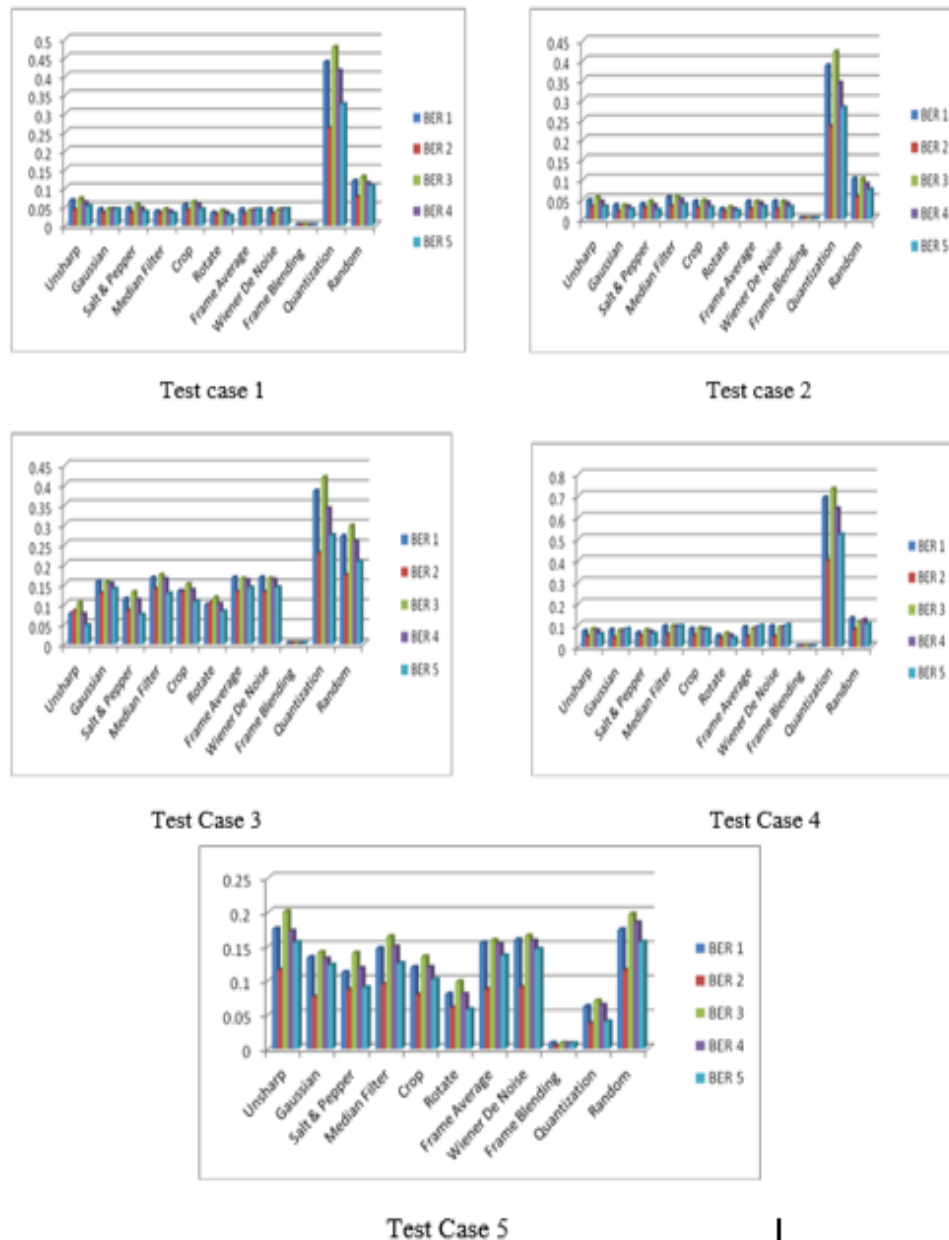


Figure 8. Histogram Representation for Various Attacks

References

- [1] M. Kumar and A. Hensman, "Robust Digital Watermarking using Reversible data hiding and Visual Cryptography", a thesis submitted for the degree of Master of Science at Institute of Technology Blanchardstown (ITB), Dublin, (2013).
- [2] F. Mintzer, G. Braudaney and M. Yeung, "Effective and Ineffective Digital Watermarks", In proceedings of the International Conference on Image Processing, IEEE Computer. Society, vol. 3, (1997), pp. 9-12.
- [3] A. H. M. Kumar, "Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography", in the Proceedings of Irish speech and signal conference (ISSC 2013), Letterkenny, Ireland, (2013) June.
- [4] T. A. Khatib, A. A. Haj, L. Rajab and H. Mohammed, "A Robust Video Watermarking Algorithm", Journal of Computer Science, vol. 4, no. 11, (2008), pp. 910-915.
- [5] L. Yen, "Digital Video watermarking robust to geometrical attacks and compression", Ottawa, Canada: A thesis submitted in the requirement of degree of Doctorate of Philosophy, (2011).
- [6] V. K. Agrawal, "Perceptual watermarking of digital video using the variable temporal length 3D-DCT", Kanpur, India: A Thesis Submitted for the Degree of M. Tech. at IIT Kanpur, (2007) June.
- [7] G. C. Langelaar, I. Setyawan and R. L. Lagendijk, "Watermarking Digital Image and Video Data: A State-of-the-Art Overview", IEEE Signal Processing Magazine, (2000), pp. 20-46.
- [8] H. Kinoshita, "An image digital signature system with ZKIP for the graph isomorphism", Lussane, Switzerland, (1996) September.
- [9] A. Dehkordi, S. Esfahani and A. Avanaki, "Robust LSB Watermarking Optimized for Local Structural Similarity", 19th Iranian Conference on Electrical Engineering (ICEE), (2011) May, pp. 1-6.
- [10] S. Patel, A. Katharotiya and M. Goyani, "A Survey on Digital Video Watermarking", International Journal of Comp. Tech. Appl., vol. 2, no. 6, (2011) December, pp. 3015-3018.
- [11] T. Kalker, J. Huitsma, M. Mues and G. Depovere, "How to Achieve robustness against scaling in Real Time Digital Watermarking system for Broadcast Monitoring", Proceedings International Conference on IEEE Image Processing, vol. 1, (2000), pp. 407-410.
- [12] C. D. Rawat and S. M. Shivamkutty, "Digital Watermarking of Video using Hybrid Techniques", in the proceeding of International Conference on Advances and Computing Technologies, (2014).
- [13] F. Hartung and B. Girod, "Digital Watermarking of MPEG-2 Coded Video in the Bit stream Domain", IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP-97, Munich, vol. 4, (1997) April, pp. 2621-2624.
- [14] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible Data Hiding", IEEE Transaction on Circuits & System for Video Technology", vol. 16, no. 3, (2006) March, pp. 354-362.
- [15] D. Lou and Chao-Lung, "Active Steganalysis for histogram-shifting based reversible data hiding", Elsevier, Journal of Optics Communication, vol. 285, no. 10, (2012), pp. 2510-2518.
- [16] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptology Eurocrypt'94 Proceedings, Springer-Verilog, vol. 950, (1995), pp. 1-12.
- [17] A. Houmansadr and S. Ghaemmagham, "A Digital Image Watermarking Scheme Based on Visual Cryptography", [Online].Available: <http://www.cs.utexas.edu/~amir/papers/IST05.pdf>. [Accessed 10 May 2013].
- [18] C. R. Babu, M. Sridhar and B. Babu, "Information Hiding in Gray Scale Images using Pseudo-Randomized Visual Cryptography Algorithm for Visual Information Security", IEEE International Conference on Information Systems and Computer Networks, (2013), pp. 195-199.
- [19] Y.-R. wang, W. H. Lin and L. Yang, "A Lossless Watermarking using Visual Cryptography Authentication", in the proceeding of the 2013 International Conference on Machine Learning and Cybernetics, Tianjin, (2013) July 14-17.
- [20] Z. Wang, A. Bovik and H. R. Sheikh, "Image Quality Assessment: From Error Measurement to Structural", IEEE Transactions on Image Processing, vol. 13, no. 4, (2004) April, pp. 600-613.
- [21] H. X. Wang and Z. M. Lu, "A modified video watermarking algorithm based on SVD in the DCT domain", International Journal of Computer Sciences and Engineering system, vol. 2, no. 1, (2008) January, pp. 37-40.
- [22] T. Y. Kuo, Y. C. Lo and C. I. Lin, "Fragile Video Watermarking Technique by Motion Field Embedding with Rate-distortion Minimization", IEEE, Vols. ISBN: 978-0-7695-3278-3, (2008) August, pp. 853-856.
- [23] H. Agarwal, R. Ahuja and S. S. Bedi, "Highly Robust and Imperceptible Luminance Based Hybrid Digital Video Watermarking Scheme for Ownership Protection", I. J. Image, Graphics and Signal Processing, vol. 11, (2012), pp. 47-52.
- [24] M. Kumar and A. Hensman, "Catalogue of Hybrid Video Watermarking Techniques", International Journal of Computer Applications (IJCAOnline) (0975-8887), vol. 143, no. 9, (2016) June.

