IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Efficient Performance of Hybrid Watermarking Scheme

Jaspreet Kaur[1], Er.Varinderjit Kaur[2], Dr.Naveen Dhillon[3]

P.G. Student, Department of CSE, RIET, Phagwara[1]

HOD, Department of CSE, RIET, Phagwara[2]

Principal of RIET, Phagwara[3]

Abstract: The digital technology enables unauthorized replica of digital images, the protection of the copyrights of digital image is a critical issue. Image watermarking schemes are used to protect the digital images. The Capacity implies total which are placed to guard image. More capacity implies one can cover wide range of information Also the watermark scrambling utilizing the Arnold transform is used to protect watermark further. Arnold transform has changed the watermark in this way that it becomes meaningless for the hackers or crackers. Different type of multiple attacks will also be considered to evaluate the effectiveness of the proposed technique. The proposed technique is designed in MATLAB tool with the help of image handling toolbox. The experiment has clearly shown that the proposed technique has better results over the available techniques.

Index terms: Watermarking Scheme, FFT, Arnold transform, SVD technique.

1. WATERMARKING SCHEME

An electronic watermark could be apparent or invisible. A visible watermark usually includes conspicuously apparent information or perhaps a company brand revealing the ownership of the image. On one other hand, an invisibly watermarked image appears much like the original.

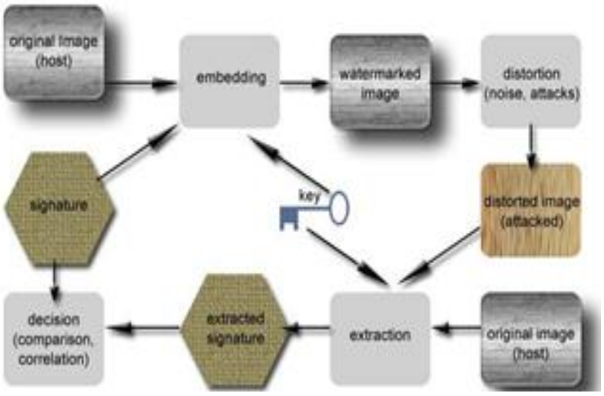


Figure 1.1: Watermarking block diagram [1]

The existence of an unseen watermark can just only be established using an suitable watermark removal or recognition algorithm. In this research we restrict our attention to invisible watermarks. An unseen watermarking process, in general, consists of an encoding process and a decoding process. Watermarks of varied number of exposure are added with display media as a guarantee of reliability, quality, possession and source.

2.TYPES OF WATERMARKING

I. In accordance with their purpose:

a) Copyright protection watermarking: This implies if the master need others to see the mark of the picture watermark, then a watermark can be seen following introducing the watermark to the picture, and the watermark still exists also if it is infected**[2].**

b) Tampering suggestion watermarking: It safeguards the reliability of the picture content, labels the altered content and avoids the usual lossy compression formats.

c) Anti-counterfeiting watermarking: It's added to the developing procedure for the paper records and can be discovered following printing, scanning, and different processes.

d) Confidential mark watermarking: It could cover essential annotation of confidential data and prohibit the illegal people to get confidential data.

II. Based on watermark type:

a) Noise type: Noise type has pseudo noise, Gaussian arbitrary and chaotic sequences.

b) Image type: You will find binary picture, press, logo and label.

III. In accordance with domain:

a) Spatial domain: This domain focuses on adjusting the pixels of one or two arbitrarily picked subsets of images. It directly loads the raw information into the image pixels. Some of its calculations are LSB, SSM Modulation centered technique.

b) Frequency domain: This strategy is also called change domain. Values of certain frequencies are modified from their original**[3]**. There are numerous frequent used change domain practices, such as FFT, DCT, DWT, and DFT.

IV. In accordance with recognition method:

a) Visual watermarking: It needs the original information in the screening class, it's stronger robustness, but its application is limited.

b) Semi blind watermarking: It generally does not involve a genuine media for recognition **[4]**.

c) Blind watermarking*:* It does not need original information, which includes large application field,
but needs a higher watermark technology

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

V. According to use of secrets:

a) Asymmetric watermarking: This is strategy where different secrets are used for embedding and detecting the watermark.

b) Symmetric watermarking: Here same secrets are used for embedding and detecting the watermark.

3.ARCHITECTURE OF IMAGE WATERMARKING

Electronic watermarking hides the copyright data in to the electronic information through particular algorithm. To track illegal copies, a unique watermark is required based on the place or identification of the receiver in the media network. The type of data concealed in them when working with watermarking is generally a signature to symbolize source or ownership for the objective of copyright protection. The key request of watermarking is copyright control, where a graphic manager attempts to prevent illegal copying of the image. Robust watermarks are properly matched for copyright security, because they live unchanged with the picture under different manipulations. An electronic watermark may be obvious or invisible. A visible watermark generally includes a plainly obvious message or even a organization brand revealing the ownership of the image. On one other give, an invisibly watermarked picture seems much like the original. The existence of an invisible watermark can only be decided using an suitable watermark extraction or detection algorithm. In this record we restrict our focus on invisible watermarks. A watermarking process is divided in to three specific measures, embedding, attack and detection**[5]**. In embedding an algorithm accepts the host and the data to be stuck, and creates a watermarked signal.

The watermark insertion step is represented as:

$$X0 = EK(X; N)$$

wherever *X* is the first image, *N* could be the watermark information being stuck, *K* could be the user's insertion crucial, and *E* presents the watermark insertion function and the watermarked variant is represented as *X0*. Relying in route the watermark is placed, and with regards to the nature of the watermarking algorithm, the detection or extraction approach may accept very specific approaches.

Watermark extraction operates the following:

$$\hat{}R = MK0(\hat{}X\ 0)$$

wherever $\hat{}X\ 0$ is just a probably corrupted watermarked image, *K0* could be the extraction crucial, *M* presents the watermark extraction/detection function, and $\hat{}R$ could be the removed watermark information.

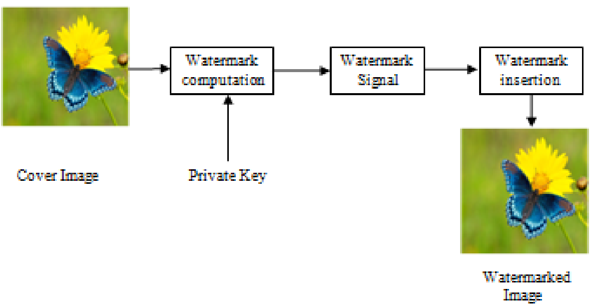


Figure 1.2: Watermark Embedding Process

Figure 1.2 shows the watermark embedding process in which original watermark is embedded in cover image by using embedding algorithm and the secret key. The image in which watermark image is inserted is called watermarked image. This watermarked image hides data because of its security purposes.

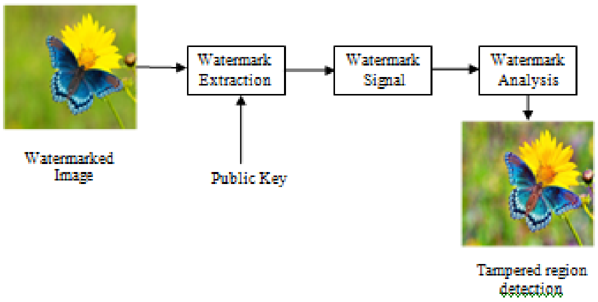


Figure 1.3: Watermark Detection Process

Figure 1.3 shows the watermark detection process in which the embedded watermark is recovered by using the detection algorithm and by using secret key. Finally the watermark signal is obtained. After watermark analysis, the tampered region is detected as output.

4. ATTACKS APPLIED

a) Sharpening Attack: Picture sharpening refers to any improvement strategy that highlights edges and fine details in an image. Picture sharpening is widely found in printing and photographic industries for raising the local contrast and sharpening the images. In concept, image sharpening contains adding to the first image a sign that is proportional to a high-pass filtered version of the first image. the first image is first filtered by way of a high-pass filter that extracts the high-frequency components, and a scaled version of the high-pass filter productivity is put into the first image, hence creating a sharpened image of the original.

b) Gamma Correction Attack: Gamma correction could be the name of a nonlinear operation used to code and decode luminance or tristimulus values in movie or however image systems. Gamma correction is, in the simplest cases, defined by the next power-law appearance: A gamma price $\gamma < 1$ is sometimes called an coding gamma, and the method of coding with this specific compressive power-law nonlinearity is called gamma pressure; alternatively a gamma price $\gamma > 1$ is called a decoding gamma and the applying of the extensive power-law nonlinearity is called gamma expansion . Gamma coding of photographs is used to improve use of bits when coding a graphic, or bandwidth used to move a graphic, by using the non-linear way people comprehend light and color. Individual vision, below common light conditions uses an approximate gamma or power function, with higher sensitivity to relative differences between deeper colors than between light ones. If photographs aren't gamma-encoded, they allocate too many bits or too much bandwidth to shows that people cannot distinguish, and not enough bits/bandwidth to shadow prices that people are sensitive to and might require more bits/bandwidth to steadfastly keep up exactly the same visible quality.

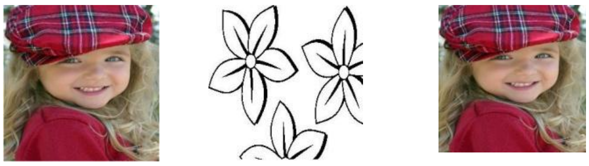
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

(c) Histogram Attack: Histogram equalization often provides unlikely consequences in photographs. It provides unwanted consequences (like obvious picture gradient) when put on images with reduced color depth. Like, if put on 8-bit picture shown with 8-bit gray-scale scheme it'll more lower color level (number of distinctive colors of gray) of the image. The histogram strike estimates a watermark by using only histogram of an image. An operation called flattering may be put on images to enhance the histogram attack. A problem of the method is that it's indiscriminate. It may increase the contrast of background noise, while decreasing the practical signal. it may also be used on color images through the use of the same process individually to the Red, Natural and Blue components of the RGB color values of the image.

5. RESULTS AND DISCUSSION



(a)Cover image **(b)Watermark image** **(c)Watermarked Image of Proposed work**

Figure 5.1: Input Images for Results

Figure 5.1 indicates the input images for experimental analysis. Fig.5.1 (a) is showing the Cover image and Fig.5.1 (b) is showing the Watermark image. The overall purpose is to combine relevant information from multiple images into a single image that's more informative and suitable for both visual perception and further computer processing. Figure 5.1 (c) has shown the watermarked image of proposed technique. Comparing the watermarked image with the original cover image does not feel the presence of the watermark. Therefore the algorithm achieves visual invisibility.

Figure 5.2: Extracted watermark of proposed technique and Effect on Watermarked image of Proposed approach without attack

Figure 5.2 has shown the extracted watermark of proposed technique without any attack. The output image contains standard SVD line in image. This line shows that only the diagonal elements are different from original watermark. In this proposed work we see the improvement in the objective quality of the image.

Another figure shows the effect on Watermarked image without any attack. In this case Watermarked image is not affected.

Figure 5.3: Extracted watermark of proposed technique and Effect of Histogram on Watermarked color Image of Proposed Technique

Figure 5.3 has shown the extracted watermark of proposed technique after Histogram attack. As diagonal elements of SVD are not effective therefore the output image contains standard SVD line on inserted watermark. In this proposed technique the objective quality of the image is improved.

Another figure has shown the effect on Watermarked image after Histogram attack. As we know that after applying attacks to Watermarked image it produces distortions in the Watermarked image. But in this case watermarked image is not affected by Histogram attack as Histogram attack allows the images to gain higher contrast by adjusting image intensities therefore image quality is improved.

Figure 5.4: Extracted watermark of proposed technique and Effect of Gamma Correction on Watermarked color Image of Proposed Technique

Figure 5.4 has shown the extracted watermark of proposed technique after Gamma Correction attack. The output image contains standard SVD line on inserted watermark as only the diagonal components being different from the original watermark image. In this proposed work there is an improvement in the objective quality of the image.

Another figure has shown the effect on Watermarked image after Gamma Correction attack. As we know that after applying attacks to Watermarked image it produces distortions in the Watermarked image. But in this case watermarked image is not affected by Gamma Correction attack as it could increase the intensity of the Watermarked image as shown. Therefore it shows an improvement in the quality of image.

Figure 5.5: Extracted watermark of proposed technique and Effect of Sharpening on Watermarked color Image of Proposed Technique

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Figure 5.5 has shown the extracted watermark of proposed technique after Sharpening attack. This image also has standard SVD line inserted on watermark which shows the diagonal elements are not effective.

Another figure has shown the effect on Watermarked image after Sharpening attack. As we know that after applying attacks to Watermarked image it produces distortions in the Watermarked image. But in this case watermarked image is not affected by sharpening attack as this attack allows the image to spotlight fine details in an image because they are created primarily by high frequency components. So the image obtained is effective.

6. PERFORMANCE EVALUATION

The proposed algorithm is tested on different images. The algorithm is applied using different performance indices Bit Error Rate (BER), Normalized cross co-relation (NCC) and Structural Similarity Index Metric (SSIM) and also the Normalized Cross Correlation is evaluated for finding out the similarities between initial watermarked image and the extracted watermarked image from the attacked image.

To be able to implement the proposed algorithm, design and implementation has been performed in MATLAB using image processing toolbox. In order to do cross validation we've also implemented partial blind watermarking scheme using DWT-sub sampling.

The developed approach is compared against some well-known watermarking techniques available in literature. After these comparisons, we're comparing proposed approach against Sharpening Attack, Gamma Correction Attack and Histogram Attack with some performance metrics. Result shows our proposed approach gives better results than the existing techniques.

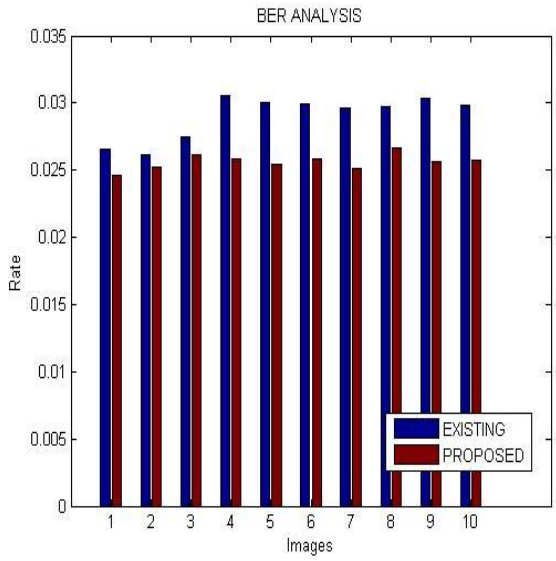
1) Bit Error Rate Evaluation

Table 6.1: Bit Error Rate Evaluation

Cover Images	Watermark Images	Existing Technique	Proposed Technique
Barbie c1	Clock w1	0.0266	0.0246
Bird c2	English w2	0.0261	0.0252
Butterfly c3	Ball w3	0.0275	0.0261
Flower c4	Teddy w4	0.0305	0.0258
Leena c5	Flower w5	0.0300	0.0254
Lake c6	Icecream w6	0.0299	0.0258
Parrot c7	Punjabi w7	0.0296	0.0251
Peppers c8	Cherry w8	0.0297	0.0267
Duck c9	Dolphins w9	0.0303	0.0256
Stones c10	Butterfly w10	0.0298	0.0257

Table 6.1shows the quantized analysis of the bit error rate. As bit error rate have to be reduced therefore the proposed algorithm is showing the better results compared to the available methods as bit error rate is less in all the cases.

Table 6.1has clearly shown that the BER is minimum in the case of the proposed algorithm therefore proposed algorithm provides better results compared to the available methods.



Graph 6.1: BER of Existing Technique & Proposed Approach for different images

Figure 6.1 shows the quantized evaluation of the bit error rate of various images using watermarking by Existing Technique (Blue color) and watermarking by Proposed Approach (Red Color).

It has clearly shown from the plot that there is decrease in BER value of images with the usage of proposed technique around other methods in all the images. This decrease represents improvement in the objective quality of the image.

2) Structural Similarity Index Metric

Table 6.2 shows the quantized evaluation of the Structural Similarity Index Metric (SSIM). As SSIM have to be maximized; so the main aim is to increase the SSIM.

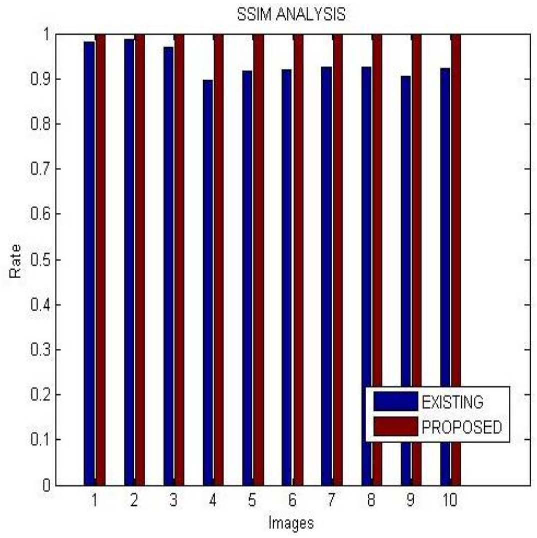
Table 6.2 has clearly shown that the SSIM is maximum in case of the proposed algorithm thus proposed algorithm provides better results compared to the avaliable methods.

Also it has clearly shown from the plot that there is increase in the SSIM values of images with the usage of proposed methods over methods. This increase represeents improvement in the objective quality of image.

Table 6.2 Structural Similarity Index Metric

Cover Images	Watermark Images	Existing Technique	Proposed Technique
Barbie c1	Clock w1	0.9813	0.9997
Bird c2	English w2	0.9859	0.9992
Butterfly c3	Ball w3	0.9707	0.9990
Flower c4	Teddy w4	0.8973	0.9992
Leena c5	Flower w5	0.9166	0.9994
Lake c6	Icecream w6	0.9205	0.9997
Parrot c7	Punjabi w7	0.9265	0.9994
Peppers c8	Cherry w8	0.9252	0.9991
Duck c9	Dolphins w9	0.9064	0.9993
Stones c10	Butterfly w10	0.9230	0.9990

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016



Graph 6.2: SSIM of Existing Technique & Proposed Approach for different images

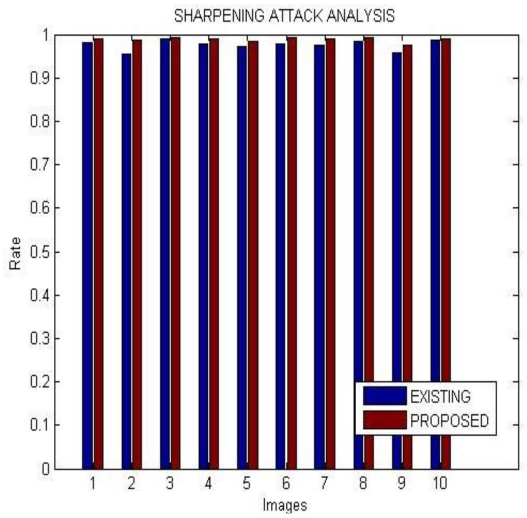
Figure 6.2 indicates the quantized analysis of the Structural Similarity Index Metric of different images using watermarking by Existing Technique (Blue Color) and watermarking by Proposed Approach (Red Color).

3) NCC Evaluation for Sharpening attack

Table 6.3 is showing the comparative analysis of the Normalized Cross-Correlation after Sharpening attack.

Table 6.3 NCC Evaluation for Sharpening attack

Cover Images	Watermark Images	Existing Technique	Proposed Technique
Barbie c1	Clock w1	0.9806	0.9900
Bird c2	English w2	0.9558	0.9856
Butterfly c3	Ball w3	0.9884	0.9935
Flower c4	Teddy w4	0.9787	0.9910
Leena c5	Flower w5	0.9712	0.9847
Lake c6	Icecream w6	0.9785	0.9915
Parrot c7	Punjabi w7	0.9749	0.9890
Peppers c8	Cherry w8	0.9850	0.9938
Duck c9	Dolphins w9	0.9583	0.9765
Stones c10	Butterfly w10	0.9870	0.9900



Graph 6.3: NCC of Existing Technique & Proposed Approach for Sharpening attack

Figure 6.3 indicates the quantized analysis of the Normalized Cross-Correlation of various images using watermarking by Existing Technique (Blue Color) and watermarking by Proposed Approach (Red Color) for Sharpening attack.

It is clear from the plot that there is an improvement in the objective quality of the image as the results are more robust than the existing techniques.

4) NCC Evaluation for Gamma Correction attack

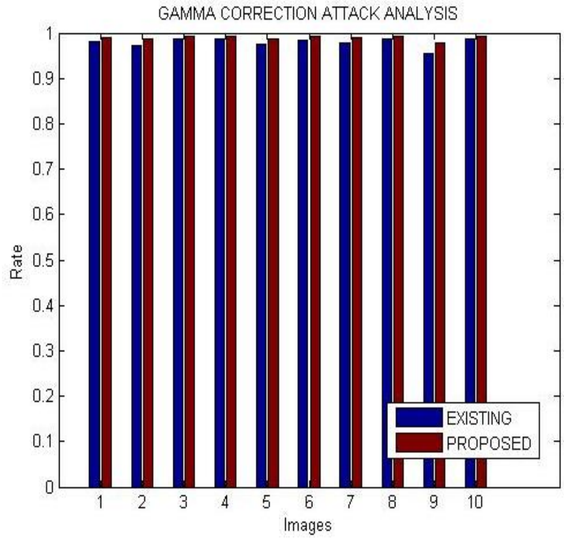
Table 6.4 is showing the comparative analysis of the Normalized Cross-Correlation after Gamma Correction attack.

Table 6.4: NCC Evaluation for Gamma Correction attack

Cover Images	Watermark Images	Existing Technique	Proposed Technique
Barbie c1	Clock w1	0.9824	0.9903
Bird c2	English w2	0.9713	0.9864
Butterfly c3	Ball w3	0.9869	0.9926
Flower c4	Teddy w4	0.9863	0.9930
Leena c5	Flower w5	0.9739	0.9867
Lake c6	Icecream w6	0.9841	0.9919
Parrot c7	Punjabi w7	0.9777	0.9901
Peppers c8	Cherry w8	0.9866	0.9939
Duck c9	Dolphins w9	0.9554	0.9773
Stones c10	Butterfly w10	0.9862	0.9914

Figure 6.4 indicates the quantized evaluation of the Normalized Cross-Correlation of various images using watermarking by Existing Technique (Blue Color) and watermarking by Proposed Approach (Red Color) for Gamma Correction attack.

It is clear from the plot that there's an improvement in the objective quality of the image as the results are more robust than the existing techniques.



Graph 6.4: NCC of Existing Technique & Proposed Approach for Gamma Correction attack

5) NCC Evaluation for histogram attack

Table 6.5 is showing the comparative analysis of the Normalized Cross-Correlation after Histogram attack.

Copyright to IJARCCE

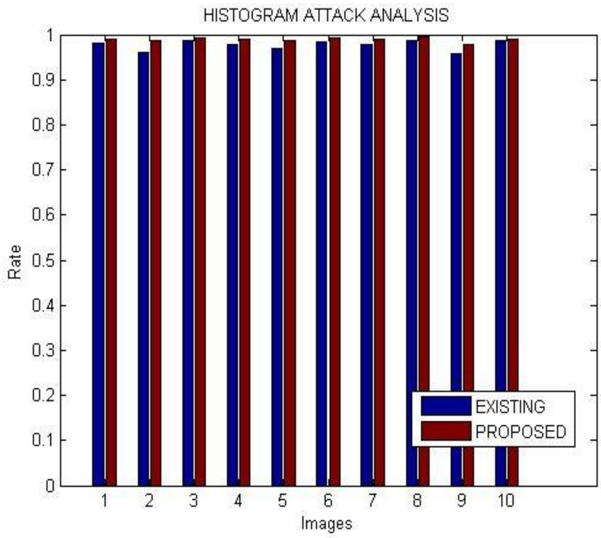
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Table 6.5 NCC Evaluation for Histogram attack

Cover Images	Watermark Images	Existing Technique	Proposed Technique
Barbie c1	Clock w1	0.9821	0.9901
Bird c2	English w2	0.9609	0.9858
Butterfly c3	Ball w3	0.9871	0.9933
Flower c4	Teddy w4	0.9785	0.9905
Leena c5	Flower w5	0.9692	0.9862
Lake c6	Icecream w6	0.9852	0.9926
Parrot c7	Punjabi w7	0.9775	0.9902
Peppers c8	Cherry w8	0.9873	0.9943
Duck c9	Dolphins w9	0.9567	0.9771
Stones c10	Butterfly w10	0.9862	0.9888



Graph 6.5: NCC of Existing Technique & Proposed Approach for Histogram attack

Figure 6.5 indicates the quantized evaluation of the Normalized Cross-Correlation of various images using watermarking by Existing Technique (Blue Color) and watermarking by Proposed Approach (Red Color) for histogram attack.

It is clear from the plot that there's an improvement in the objective quality of the image as the results are more robust than the existing techniques.

7.CONCLUSION

A low profile watermarking solution, overall, contains some sort of encoding activity plus a decoding process. Also the Arnold transform is used to safeguard watermark further. Arnold transform has changed the watermark in such a way that it become useless for the hackers or crackers. Different kind of multiple attacks may also be considered to to evaluate the effectiveness of the proposed technique. The proposed technique is designed in MATLAB tool with the aid of image processing toolbox. The experiments has clearly shown that the proposed technique outperforms over the available techniques. The experiments has clearly shown the improvement in SSIM is .89 %. Also the results in the most of the selected attacks has clearly shown that the proposed technique performs better over the available techniques.

REFERENCES

[1] Raval, Keta, and S. Zafar. "Digital Watermarking with copyright authentication for image communication." In *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, pp. 111-116. IEEE, 2013.
[2] Varghese, Justin, Omer Bin Hussain, Bijoy Babu, Jamshid M. Basheer, Saudia Subash, Mohamed Ramadan Saadi, and Mohamed Samiulla Khan. "An efficient DCT-SVD based algorithm for digital image watermarking." In *Security Technology (ICCST), 2014 International Carnahan Conference on*, pp. 1-6. IEEE, 2014.
[3] Kakkirala, Krishna Rao, Srinivasa Rao Chalamala, and Jyoti Dhillon. "A robust image watermarking using DWT, SVD and Torus automorphism." *In Computational Intelligence and Cybernetics (CYBERNETICSCOM), 2013 IEEE International Conference on, pp. 160-163. IEEE, 2013.*
[4] Zhao, Ke, and Jiang-feng Xu. "A new semi-blind watermarking scheme based on DWT-subsampling." *In Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on, pp. 623-626. IEEE, 2013.*
[5] Zhu, Yong, Xiaohong Yu, and Xiaohuan Liu. "An image authentication technology based on digital watermarking." In *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on*, pp. 179-183. IEEE, 2013.
[6] Ghaderi, Kayvan, Fardin Akhlghian, and Parham Moradi. "A new digital image watermarking approach based on DWT-SVD and CPPN-NEAT." In *Computer and Knowledge Engineering (ICCKE), 2012 2nd International eConference on*, pp. 12-17. IEEE, 2012.
[7] Guan, Hu, Zhi Zeng, Jie Liu, Shuwu Zhang, and Peiyu Guo. "A novel geometrically invariant blind robust watermarking algorithm based on SVD and DCT." In *Image Analysis and Signal Processing (IASP), 2012 International Conference on*, pp. 1-5. IEEE, 2012.
[8] Mangaiyarkarasi, P., and S. Arulselvi. "A new digital image watermarking based on Finite Ridgelet Transform and extraction using ICA." In *Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on*, pp. 837-841. IEEE, 2011.
[9] Al-Gindy, Ahmed, Hana Younes, Amira Shaleen, and Hala Elsadi, "A graphical user interface watermarking technique for the copyright protection of colour images using colour watermarks," *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp.354-358, December 2011.*
[10] Dharwadkar, Nagaraj V., B. B. Amberker, and Avijeet Gorai. "Non-blind watermarking scheme for color images in RGB space using DWT-SVD." In *Communications and Signal Processing (ICCSP), 2011 International Conference on*, pp. 489-493. IEEE, 2011.
[11] Prasad, R. M., and Shivaprakash Koliwad. "A robust wavelet-based watermarking scheme for copyright protection of digital images." *In Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on, pp. 1-9. IEEE, 2010.*
[12] Amini, Marzieh, Khashayar Yaghmaie, and Hamidreza Sadreazami. "Error diffusion halftone image watermarking based on SVD-DWT technique." *In Machine Vision and Image Processing (MVIP), 2010 6th Iranian, pp. 1-4. IEEE, 2010.*
[13] Ghosh, Sudip, Pranab Ray, Santi P. Maity, and Hafizur Rahaman. "Spread spectrum image watermarking with digital design." *In Advance Computing Conference, 2009. IACC 2009. IEEE International, pp. 868-873. IEEE, 2009.*
[14] M.A.Dorairangaswamy, "An effective blind watermarking scheme for protecting rightful ownership of digital images," *TENCON IEEE Region 10 Conference, pp. 1-6, January 2009.*
[15] Wang and Hwa-kim, "Color Image of Tamper Detection and Recovery Using Block-Based Watermarking Embedded and Multimedia Computing", 2009. EM-Com 2009. 4th International Conference IEEE, pp. 1-6, Dec. 2009.
[16] X. Changzhen, G. Fenhong, and L. Zhengxi, "Weakness analysis of singular value based watermarking," *in Mechatronics and Automation, 2009. ICMA 2009. International Conference on, 2009, pp. 2596–2601.*
[17] Bhatnagar, G. and Raman, B., "A new robust reference watermarking scheme based on DWT-SVD", Elsevier B.V. 2008.