IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Multiple Image Hiding Using Arnold Transformation

Vinjamuri Roopaswi[1*], V.V. Hari Babu[2]

[1]Dept. of Computer Science and Engineering, Bapatla Engineering College, Guntur District, India
[2]Dept. of Physics, Bapatla Engineering College, Guntur District, India

Corresponding Author: vroopaswi@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i5.295299 | Available online at: www.ijcseonline.org

Accepted: 16/May/2019, Published: 31/May/2019

***Abstract*:** Dct and Arnold transform is used for a procedure called encryption where encryption is a process of adding extra bits top the information which can be read by the end to end sender and receiver.
Example of encryption can defined as let's consider a sentence ''there code is 100052'' this is very confidential which should be known only to two persons which is sender and receiver. Here sender adds some information using some algorithms and the sentence becomes 'thereacodeaisa1a0a0a0a5a2' or a by using a circuit called encoder. The same when the receiver uses the same encoded algorithm to remove the extra bits added here is the original data is obtained by using decoder circuit which performs the inverse operation of that of encoder. To hide the information or a string were a image consists of 4 parts by applying the 2nd level LWT. Low frequency sub bands LL2 and LH2 are then converted by DCT. And the 2 image are converted using DCT and again one of the converted image is the n again applied to ARNOLD. The output of Arnold is the water marked image.

***Keywords*:** RDWT and SVM, Watermarking, Encoding.

I. INTRODUCTION

A wide range of technologies for end-to-end protection are needed to resist the security threats in modern communication. For present business trends, digital media plays a significant part and also there comes the need of securing the data/information from unauthorized personals. For achieving this, the secured Personal information should be embedded in to digital content which is conjoined by nature. This concept of protecting the information is called as watermarking. The key property of watermarking is its robustness to any kind of attacks which in turn makes it impossible to separate the watermark without disturbing or degrading content.. Digital watermarking, steganography and Reversible Data Hiding are methods used.

Data hiding is performed by some assistant, when the owner doesn't trust the assistant or an admin completely. Then this watermarking technique comes in to picture. Where an secret image is added in order to protect the copyright value provided by the owner . Where owner can add a concept of encryption where bits are added and now images are added. Encryption can defined as let's consider a sentence ''there code is 100052'' this is very confidential which should be known only to two persons which is sender and receiver. Here sender adds some information using some algorithms and the sentence becomes 'thereacodeaisa1a0a0a0a5a2' or a by using a circuit called encoder. The same when the receiver uses the same encoded algorithm to remove the extra bits added here is the original data is obtained by using decoder circuit which performs the inverse operation of that of encoder

When the owner performs watermarking the data whose owner ship remains non conflicts because only the owner knows the key to remove the watermark so the owner can provoke the copyright permission whom the owner owns the full copy right protection of the data or the picture
.

II. LITERATURE SURVEY

M. Khalili, D. Asatryan [10] : The most digital image watermarking algorithms have nearly invariably been complete in red, inexperienced and blue (RGB) color area. during this study, a secure, strong and inaudible CDMA image watermarking theme that uses separate wave rework is projected and tested in eight color areas RGB, YCbCr, JPEG-YCbCr, YIQ, YUV, hue, saturation, intensity, hue, saturation, worth and CIELab to see that color area is simpler in watermarking algorithms supported correlation techniques and provides a result which doesn't take issue infinitely from the first with relevancy physical property and lustiness. Within the projected theme, a disorganized binary image by Arnold rework map, once secret writing, is embedded into sub-images of the primary channel wave decomposition of supposed color area victimization block process technique. The experimental results show that the projected approach provides further physical property,

security and lustiness against JPEG compression and totally different noise attacks compared to the similar projected ways in earlier works.

R. Zhang, Y. Wang [5]: With DCT and HVS, this paper proposed a frequency domain image watermarking algorithm based on mapping principle in Toral Automorphism. Firstly, we scrambled the original watermark image with Arnold transformation. Secondly, we transformed the original carrier image by discrete cosine transformation and chose some proper intermediate frequency coefficients based on human visual system. Thirdly, the processed watermark was embedded into these coefficients with spread-spectrum mechanism. Finally, the watermark was extracted by the blind detection and recovered by periodic Arnold transformation, which could authenticate digital works and protect the copyrights. The algorithm has the advantages of robustness and security with scrambling transformation and spread-spectrum techniques, invisibility with HVS features.

F. Ernawan, M. N. Kabir, J. M. Zain[11]: Compressing an image can reduce thre storage space in this paper the whole method is been described by setting threshold and some ideas of audio coding and resource allotment is been done. It deals with image frequency coding and local block alignment it deals with eliminating the degraded part present in the images where the unwanted components are removed to make the visual appearance nice as possible

III. EXISTING METHOD

The proposed methodology for Watermark embedding is illustrated in Fig. 2 and fully described in this section.

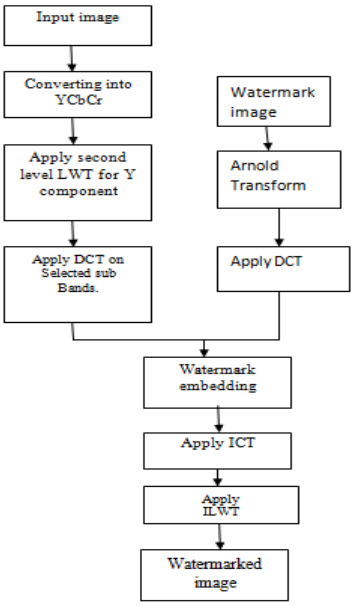


Figure-2: Block diagram of the Watermarking embedding process

1. Convert an RGB cover image to YCbCr image and choosing Y region for embedding the watermark.
2. Apply second-level LWT to decompose the Y region into their corresponding four sub bands. Select LL2 sub-band.
3. Apply DCT over selected sub-bands LL2.
4. One out of two watermarks is encrypted using the Arnold transformation and second is used directly. Then both watermarks are transformed using DCT.
5. In this step, embedding of both the watermarks is performed. The encrypted watermark is embedded into LL2 band by following equation. WLL2= OLL2+ K*Tw1. Where OLL2 is the DCT transformed LL2 sub band of original image, K is gain factor of the watermark and Tw1 is the DCT transformed encrypted watermark image.WLL2 is the watermarked image
6. Obtain modified W*LL2 sub band by applying inverse discrete cosine transformation (IDCT) over the LL2 sub band of watermark embedded image co-efficient.
7. Replace LL2 sub band of cover image with the W*LL2 sub band and apply Inverse LWT to combine all the four sub-band together.
8. Concatenate all the three components of image i.e. modified Y, Cb and Cr to get the RGB watermarked image.

Discrete Cosine Transform (DCT):
DCT is one of most popular technique used in digital watermarking . DCT turns image from spatial domain to frequency domain.DCT transforms the image into three frequency bands as lower, middle and higher frequency bands. Middle frequency bands are preferred due to less vulnerability towards attacks. It gives better results against attacks like cropping, sharpening and has better efficiency..

Lifting Wavelet Transformation :
LWT is fast and efficient way of transforming an image. Lifting technique is known to be second generation of wavelet transformation. LWT is lifting scheme based on discrete wavelet transformation. It comprises of three stages split, predict and update. LWT is better than traditional wavelet transformation as it reduces the computational time and memory requirement.

Arnold Transformation:
Arnold transformation is famous image encryption method but its scope is limited to square size images like M x M. Arnold method is also known as image scrambling method It is widely used in image watermarking due to its periodicity property. Arnold period implies that number of Iteration depends on size of image. After peak, the original image starts to reappear due to degradation in the encryption like bell shape curve. Arnold transformation. Arnold transformation is basically a image scrambling method. It provides more security to watermark and the information highly important can be transformed using this method

WATERMARK EXTRACTION:

Algorithm: Procedure for Extraction of image used for Watermarking

1. Convert an RGB watermarked image to YCbCr image and choose Y region for extracting the watermark.
2. Apply second-level LWT transformation to decompose it into corresponding 4 sub bands and select LL2 sub-band.
3. Apply DCT to selected sub bands and obtain corresponding transformed coefficients.
4. Apply steps (1),(2) and (3) to cover image to obtain their corresponding DCT transformed values for sub band LL2 .

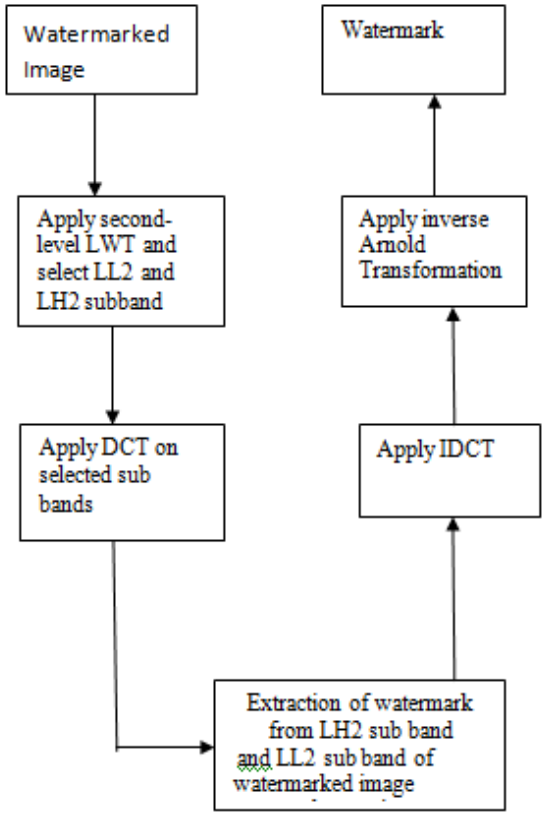


FIG:3 **:** Block diagram of the Watermarking Extraction process

5. Obtain DCT transformed values using (W*LL2- OLL2)/k = Tw1 and (W*LH2- OLH2)/k = Tw2 for both the sub bands.
6. Apply inverse DCT over extracted watermarks Tw1 and Tw2 respectively and as a result we get Tw1 in encrypted format and Tw2 as original watermark.
7. Apply inverse Arnold transformation on Tw1 to get the original watermark.

IV. PROPOSED METHOD

There are two algorithms used for water marking technique for 2 image water marking.

Algorithm for adding watermark

1. take one image which red, blue, green components and convert it to YCBCR format and then take only the Y components to process the image
2. apply second level lwt to process the Y region of image . select LL2 and LH2 bands
3. apply DCT for LL2 and LH2
4. one output of those two image is given as input to Arnold transformation. After Arnold transformation the remaining output and the Arnold transformation output is processed by using DCT.
5. In this step, embedding of both the watermarks isperformed. The encrypted watermark is embedded intoLL2 band and other watermark in LH2 band using thefollowing equation.
   WLL2= OLL2+ K*Tw1 and WLH2= OLH2+ K*Tw2 respectively. Where OLL2 is the DCT transformed LL2 sub band of original image, K is gain factor of the watermark and Tw1 is the DCT transformed encrypted watermark image.WLL2 is the watermarked image. Where OLH2 is the DCT transformed LH2 sub band of original image, K is gain factor of the watermark and Tw2 is the DCT transformed
   watermark image.WLH2 is the watermarked image.
6. Obtained modified sub bands by applying inverse discrete cosine transformation (IDCT) over the LL2 and LH2of watermark image coefficient
7. Replace LL2 and LH2 of image with W*LL2 and W*LH2 sub bands and aply LWT to combine all four sub-bands together
8. Merge all the 3 components of image with modified y,cb and cr to get the RGB watermarked image

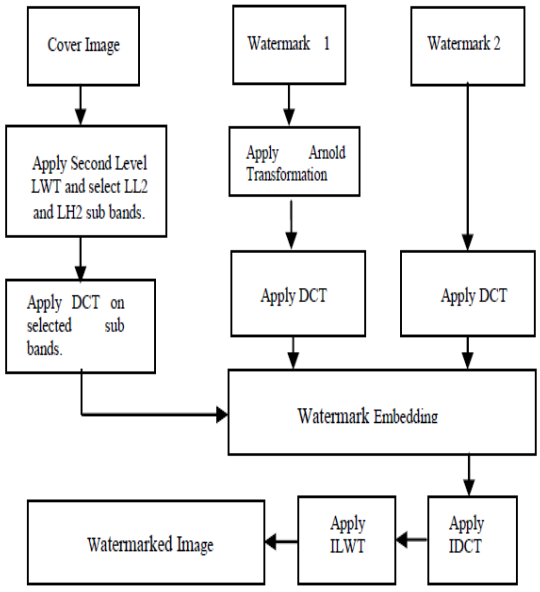


Figure 2: (a) Watermark embedding Process

Watermark extraction algorithm

9. Convert rgb to ycbcr and choose only y region for extracting the watermark

10. Apply second-level LWT transformation to decompose in 4 bansds and a take only 2 bands LL2 and LH2 bands
11. DCT is applied to selected bands to obtain required outputs
12. Apply (9),(10),(11) to cover image to obtain their DCT transformed values for sub bands LL2 and LH2
13. Obtain DCT transformed values using (W*LL2-OLL2)/k=Tw1 and (W*LH2-OLH2)/k=TW2 for both sub bands
14. Apply idct and TW1 in encrypted format and TW2 as original watermark
15. Apply inverse Arnold transformation on Tw1 to get the original watermark

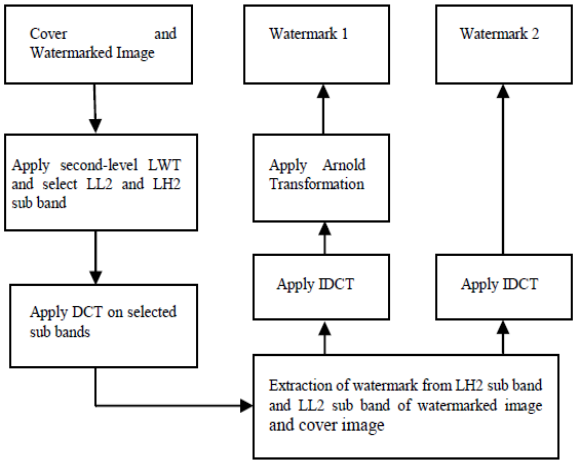
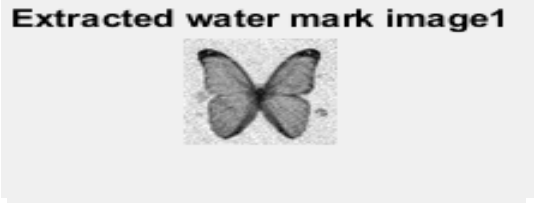


Figure 2: (b) Watermark extraction Process

Applications

- Used for image copyright protection in photo studios
- Used in Examination department for security applications

V. RESULTS



VI. CONCLUSION

In this paper, an efficient approach based on LWT and DCT is presented along with Arnold transformation to provide secure watermarking. The concepts of two watermarks are used in the cover image. Embedding of multiple watermarks in the cover image reduces the consequences of illegal usage. One of the two watermarks is encrypted using Arnold transformation and embedding in selected sub bands is discussed in the paper. The proposed algorithm is fast and efficient technique and provides better result than other wavelet transformations which were proposed earlier. The combination of LWT, DCT and Arnold provides more secure watermarking.

REFERENCES

[1] N. Otsu, "A threshold selection method from gray-level histograms," IEEE Transactions on Systems, Man, and Cybernetics, vol. 9, no. 1, pp. 62–66, 1979.

[2] J. Kapur, P. Sahoo, and A. Wong, "A new method for gray-level picture thresholding using the entropy of the histogram," Computer Vision, Graphics, and Image Processing, vol. 29, no. 3, pp. 273–285, 1985.

[3] W. Niblack, An introduction to digital image processing. Englewood Cliffs: Prentice Hall, 1986.

[4] J. Sauvola and M. Pietikäinen, "Adaptive document image binarization," Pattern Recognition, vol. 33, no. 2, pp. 225–236, 2000.

[5] B. Gatos, I. Pratikakis, and S. Perantonis, "Adaptive degraded document image binarization," Pattern Recognition, vol. 39, no. 3, pp. 317–327, 2006.

[6] D. Bradley and G. Roth, "Adaptive thresholding using the integral image," Journal of Graphics Tools, vol. 12, no. 2, pp. 13–21, 2007.

[7] C. Wolf and J.-M. Jolion, "Extraction and recognition of artificial text in multimedia documents," Formal Pattern Analysis & Applications, vol. 6, no. 4, pp. 309–326, 2004.

[8] M.-L. Feng and Y.-P. Tan, "Adaptive binarization method for document image analysis," in Proc. 2004 IEEE International Conference on Multimedia and Expo (ICME), vol. 1, June 2004, pp. 339–342.

[9] M.F. M. El Bireki, M. F. L. Abdullah, Ali A. M. Ukasha and Ali A. Elrowayati , "Digital Image Watermarking Based On Joint (DCT-DWT) and Arnold Transform" in International Journal of Security and Its Applications Vol. 10, No. 5 , pp.107-118,2016.

[10] Vivek Singh Verma , Rajib Kumar Jha, "Improved watermarking technique based on significant difference of lifting wavelet coefficients" in Springer ,2014. DOI 10.1007/s11760-013-0603-6.

[11] Sushma G. Kejgir, Manesh Kokare, "Lifting Wavelet Transform with Singular Value Decomposition for Robust Digital Image Watermarking " in International Journal of Computer Applications · February 2012.Document Recognition and Retrieval XVI, vol. 7247, 2009, pp. 7247– 7247–9.

[12]L. P. Saxena, "Niblack's binarization method and its modifications to real-time applications: a review," Artificial Intelligence Review, pp. 1–33, 2017.

[13] R. F. Moghaddam and M. Cheriet, "AdOtsu: An adaptive and parameterless generalization of Otsu's method for document image binarization," Pattern Recognition, vol. 45, no. 6, pp. 2419–2431, 2012.

[14] C.-H. Chou, W.-H. Lin, and F. Chang, "A binarization method with learning-built rules for document images produced by cameras," Pattern Recognition, vol. 43, no. 4, pp. 1518–1530, 2010.

[15] V. Kulyukin, A. Kutiyanawala, and T. Zaman, "Eyes-free barcode detection on smartphones with Niblack's binarization and Support Vector Machines," in Proceedings of the 16th International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV'2012) at the World Congress in Computer Science, Computer Engineering, and Applied Computing WORLDCOMP, vol. 1. CSREA Press, 7 2012, pp. 284–290.

