Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Hybrid Digital Watermarking Technique using AES Encryption

Diksha Kumari [1], Vishal Shrivastava [2], Akhil Pandey [3]
Department of Computer Science and Engineering
Arya College of Engineering and I.T., Jaipur

***Abstract*— During the current year every industrial application is on the way of computerized period, due to a huge improvement in most recent advances, for example, in the territory of correspondence, organized sight and sound framework, advanced information stockpiling and so on. Because of the addition in the progression in the field of digitalization and the developing the worry of the people towards the viability, security, the things has changed over the most recent two decades where the contribution of web in business industry has expanded. For a situation on which the web is concerned it is the accumulation of information in different structures like printed, sound, video, for which the responsibility for information is should have been secured. Watermarking is being characterized as the way toward ensuring the information accessible on the web or disconnected from the adapting and furthermore the unapproved access to the information is considered. In this work the significant consideration is being considered for the presentation and furthermore for the security related worries of the watermarking procedure for which DWT, DCT and SVD is being utilized and for the encryption procedure AES is utilized.**

Index Terms*— Digital watermarking, Encryption, Decryption, Image, Textual, Cryptography.

I. INTRODUCTION

By a couple of years ago, web turned into the main need of everybody. It is an exceptionally simple and quick approach to move and access information and data all through the world. This data is essential as computerized information (content, pictures, sound, video). Everybody utilizes web for their own or expert usage. Because of this it is essential to shield client information from unapproved get to. At the time we mentioned about duplicate right insurance implies unapproved individual case that replicated information is made by him. Watermarking is being characterized as the way toward securing the information accessible on the web or disconnected from the adapting and furthermore the unapproved entrance to the information is well thought-out.

For the situation when the computerized information is coordinated with the watermarks, the procedure is named as the advanced checking. The information that is hidden is watermark and the equivalent is inserted with the other type of information like sound, video or even content can be considered for installing [1]. Advanced watermarking is of two sorts as unmistakable and undetectable watermarking. The portion of advanced watermarking is particularly connected with the idea of the steganography [2].

Steganography is characterized as the idea of secured composing, where the basic printed information is being stored secretly utilizing some other media and the advanced watermarking is being characterized as the way toward concealing the mystery writings, so the information can be better ensured and furthermore the un-approved can be confined. The watermarks which are installed are very difficult to evacuate and are simply indistinct and furthermore the spread media or the watermark can be of any sort like content, sound, video, and so on. The degree of intangibility can't be characterized on account of the computerized watermarking. Because of the watermarking the extricated information might be of less quality as it initially seemed to be. To beat this restriction and to recover the first information, reversible watermarking has been actualized which is considered as a best methodology available on the cryptography.

For defeating this issue Digital watermarking system is utilized in as to shield information from illicit duplicates or unlawful conveyance. It is a craft of concealing data into advanced information as it were; unapproved individual can't access or duplicate that information for abuse. Information which is embedding into advanced media is called watermark. It is a data (any name, references, creator name, id) related to the information.

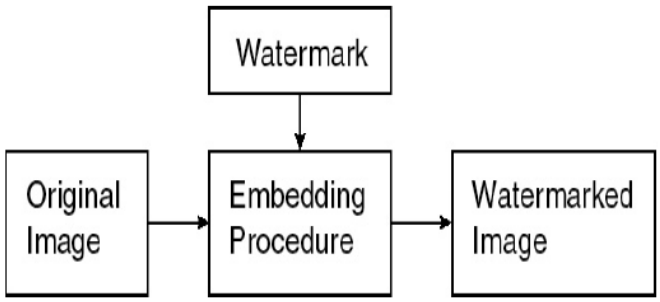

Fig. 1 Watermarking Algorithm general form.

II. PROCEDURES USED IN PROPOSAL

A. DWT

[3] During the implementation of this method of watermarking picture is subdivided into four sections. These are as level part, corner to corner part, vertical part, and guess part. The picture is separated into four sections for changing over the picture into low goals picture. The procedure is rehashed for figuring the different scale wavelet disintegration. DWT is progressively best strategy for watermarking in light of the fact that it performs calculations in all respects precisely. The positive purpose of this method is that it is hearty to deal with the commotion in the picture. DWT has come about as one of the incredible asset for the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

properly handling of the sign in a considerable lot of the utilizations of the different fields like pressure of sound media, acknowledgment of various examples, separation of surface, PC designs, and so on. There are likewise different forms of DWT are accessible like 2-D DWT and 2-D Inverse DWT which are being considered as the partners of each other which functions admirably on account of a large number of the uses of coding for picture and video.

B. DCT

[4] This represents Discrete Cosine Transform. Primary component of utilizing this system is that it gives the great sign estimation by utilizing certain coefficient esteems. This method is utilized by numerous calculations for implanting the watermarking on picture. The principle preferred position of this system is that it is very quick as contrast with different methods. In this method the watermark is installed on the inside recurrence groups as a result of decay of the picture. This strategy is progressively strong to lossy compressions as contrast with others.

C. SVD

[5] The utilization of SVD is done for breaking down the measurements in the numerical manner. The networks are changed into three sub-lattices utilizing the idea of SVD and the size of recovered grids is only same as of the first matric. According to the thought of the straight variable based math, a picture is considered as the variety of scaler sections which are non-negative and can be considered as the network. Considering the An as the squaring picture, spoke to as A Ɛ R^{nxn}, where R depicts thedomains real numbers, at that point SVD of An is characterized as A=USVT where U and V are symmetrical lattices, and S is a slanting grid, as

$$S = \begin{bmatrix} s_1 & & \\ & \ddots & \\ & & s_n \end{bmatrix}$$

At this point askew components for example s' are solitary qualities and fulfill $S_1 \geq S_2 \geq \ldots S_r \geq S_{r+1} \geq = \ldots\ldots = S_n = 0$.

An ideal grid disintegration method is SVD in a least square sense that it packs the most extreme sign vitality into as couple of coefficients as could reasonably be expected.

III. LITERATURE REVIEW

During his study author proposed a strategy where two distinct calculations are combined, method for watermarking and encryption system for which AES [6] is considered. Cryptography is being utilized with the end goal of simply scrambling the message and the equivalent being known at the season of correspondence. The mystery information in being hided inside the figure, the harm is being finished by the block attempt in light of the way that it is known to aggressors that there is correspondence between the source and goal. On account of the strategies of steganography the data that demonstrates that the correspondence is going on is additionally kept secret [7].

During the explanation the creator has thought about the advance watermarking of DWT, DCT and SVD for the proposition of the upgraded method for watermarking. In the extremely next area the creator attempts to speak to the phases of watermarking and furthermore of extraction process, for the extraction procedure the creator have utilized the idea of flowchart. The implanting procedure and extraction process really demonstrates how the installing of the watermark picture is being finished with the spread picture and again how the first picture is separated back [8].

During recent time Preeti Parashar [9] et al, mentioned in general information goes over the web with the end goal of correspondence. In this manner the security of advanced information is the principle concern. In this creator characterizes, that computerized watermarking is a method which is utilized to verify the classified information. It keeps the information from duplication or altering by concealing the mystery message in the first data or information. The areas sorted the procedure of picture watermarking as spatial space; change area and so on spatial space is a strategy which deals with the premise of pixels. Also, the space, recurrence area takes a shot at the change coefficients o the picture. During this paper creator centres around the spatial and change area alongside their favourable circumstances and drawbacks.

During the implementation of this paper it is characterized that Digital watermarking is a procedure to conceal the information behind any picture, sound, video and so forth by Vinita Gupta [10] et al. It is a type of cryptography. In this paper picture watermarking is clarified. Diverse systems are likewise examined for picture watermarking. Utilizations of picture watermarking are likewise characterized. A few elements and properties are additionally talked about alongside a review performed in New York based on picture watermarking.

In this paper a procedure is projected to ensure advanced character records against a Print Scan assault for a verified ID card validation framework that is presented by Peyman Rahmati, Andy Adler and Thomas Tran, ―Watermarking in E-trade [11]. The current PS activity forces a few twists, for example, geometric pivot and histogram bending on the watermark area which may cause the loss of data. The proposed framework expels mutilation of the PS activity: - separating, restriction, binarization, turn and editing. The proposed confirmation framework removes the watermarks inside the ID card's holder photograph, place in the decoder and afterward looks at it with the ID card individual number. On the off chance that the removed watermark and the ID card individual number are the equivalent, the character of the user/client will be checked generally personality will be deprived of.

IV. PROBLEM STATEMENT

During the above research work, for the watermark conspire we will utilize the DWT, DCT and SVD with AES calculation. DWT is a standout amongst the most famous watermark plot so in this work we use DWT and for increment the presentation we likewise use DCT and SVD as cross breed watermarking procedure and encryption calculation to improve the security parameter. Every security and testing parameters will be properly elaborated in this work.

In this research investigation an Advanced Encryption Standard Algorithm (AES) is being utilized with the end point

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

goal of encryption of the information which is being transmitted over the web. AES is standard square figure method and is very productive when contrasted with the DES (Data Encryption Standard) procedure. The term square figure demonstrates that the procedure works over the characterized size of the information squares and furthermore results the yield square of same size as information square. In AES system an info key is being utilized. The phase of choice of the task mode is about the determination of the particular execution of the AES calculation. The info square of information is of size 128 bits.

V. PROPOSED WORK

In the examined work, for the reason for watermarking DWT [19], DCT [20] and SVD [21] is being utilized for the inserting procedure and in favor of the AES [22] is additionally being utilized alongside the other talked about systems with the end goal of the extraction of the objective picture. DWT is being considered as one of the ground-breaking and a standout amongst the most productive apparatus of the watermarking procedure and for expanding the exhibition of the total procedure DCT and SVD which results as the half breed watermarking method. The encryption system is being for expanding the security level of the information and of the parameters too.

During the proposed strategy AES (Advanced Encryption Standard Algorithm) is being utilized for the encryption of the picture that is to be broadcasted utilizing some computerized medium. AES depends on standard square jaunty idea implies, in the system the size of the information square is pre-characterized and furthermore the size of the yield will dependably be equivalent to that of the info. In the AES system the information key is given as contribution to the calculation. The method of activity really characterizes the choice of the execution of the AES procedure. The size of info square which really is pre-chosen is well thought-out of size 128 bits.

An advanced watermarking technique is alluded to because spread-range if the checked sign is acquired by an added substance alteration. Spread-range watermarks are known to be unobtrusively powerful, yet in addition to have a uninformed limit because of host impedance.

An advanced watermarking technique is supposed to be of quantization type if the stamped sign is gotten by quantization. Quantization watermarks experience the ill effects of low strength however have a high data limit because of dismissal of host impedance. An advanced watermarking strategy is alluded to as sufficiency regulation if the checked sign is implanted by added substance alteration which is like spread range technique yet is especially inserted in the spatial space.

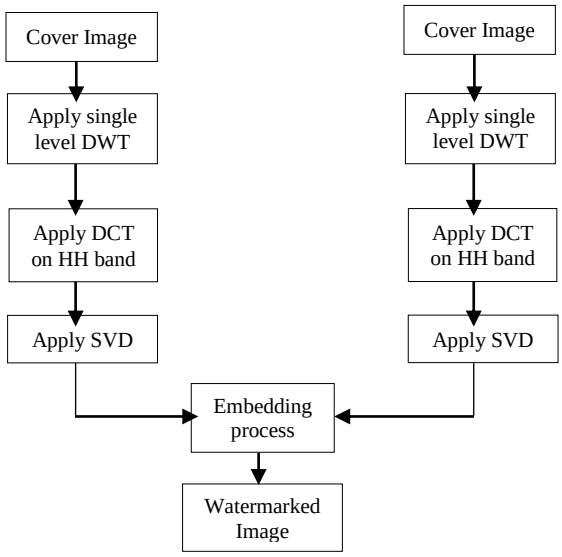

Fig. 2 Embedding Process.

Fig. 3Transmission Phase.

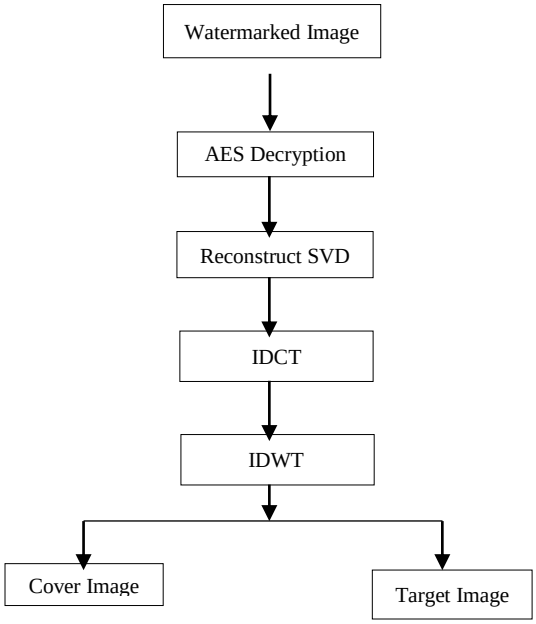

Fig. 4 Extraction Process.

PROCEDURE OF EMBEDDING

⇒ ***Step 1:*** Two unique pictures are considered as contribution as spread (picture utilized for stowing away) and target picture (that is to be unseen),

⇒ ***Step 2:*** Single level DWT is being connected on the objective picture and spread picture independently,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

⇒ ***Step 3:*** Implement DCT over the HH band created by DWT method over the objective picture and spread picture,

⇒ ***Step 4:*** SVD is connected on the DCT pictures created from DWT over spread pictures and target pictures.

⇒ ***Step 5:*** The SVD pictures are then inserted and scrambled for better security and confirmation, for the encryption AES strategy is being utilized,

⇒ ***Step 6:*** The yielding of the inserting procedure is the watermarked picture which is hided inside the spread picture and the equivalent is being scrambled by AES algorithmic calculation,

PROCEDURE OF EXTRACTION

⇒ ***Step 7:*** Watermarked picture is being considered as the contribution to the extraction procedure,

⇒ ***Step 8:*** Decryption procedure is done to get the inserted picture utilizing the AES algorithmic calculation,

⇒ ***Step 9:*** SVD images is remade back, independently as spread and target picture,

⇒ ***Step 10:*** IDCT (Inverse Discrete Cosine transform is connected to get the DCT spread and target pictures),

⇒ ***Step 11:*** In the same way, IDWT (Inverse Discrete Wavelet Transform is connected to acquire the spread picture and target pictures),

VI. RESULT AND DISCUSSION

The proposed methodology is taken in to utilization MATLAB 2015a at Intel double center processor CPU 1.6 GHz PC with 4 GB of RAM. The outcomes are clarified by discovering all the recovered significant data by assessing the MSE, PSNR, security, computational overhead, productivity and so forth. The exploratory consequences of existing methodologies dependent on other methodology and proposed approach are portrayed as table. At last, the discoveries of the all tested framework will be talked about and broke down.

For checking the proposed methodology the dataset utilized that contains the accompanying areas:

- A set of target images
- A set cover images

The presentation of the proposed work was evaluated by this dataset; in this objective picture inserted by spread picture and scrambled with AES calculation; entire procedure is singular premise in the part of target picture.

In case of computing the importance of the proposed methodology numerous parameters are utilized for the assessment of results. Following are the parameters:

- MSE (Mean Square Error)
- PSNR
- Efficiency
- Communication overhead
- Computational overhead
- Key Size
- Data Sharing
- Security.

TABLE I QUANTITATIVE RESULT ANALYSIS.

Image	MSE	PSNR
RTU logo	220.64	264.91
Pepsi	222.96	23.48
Copy right	298.32	265.64

TABLE II PERFORMANCE COMPARISON EXISTING WORK AND PROPOSED WORK.

Parameters	Existing Work(s)	Proposed Work
Efficiency	Average	High (due to hybrid watermarking)
Computational overhead	Average	Average (But compare to existing it increase due to the hybrid and encryption phase)
Communication overhead	Same	Same (no change at transmission phase)
Key Size	Depend on the approach (Nil, Average, High)	Average (AES encryption)
Security	Average	High (due to hybrid and encryption mechanism)
Data Sharing	Allow	Allow

It is very well observed from the table II that proposed work expands the security on picture with its proficiency and respectability. The estimation of security is more prominent than the current methodology. It might be conceivable that the computational overhead is increment however the security parameter is progressively significant issue w.r.t. these parameters on classified information and pictures.

The snapshots in stepwise way are demonstrated as follows:

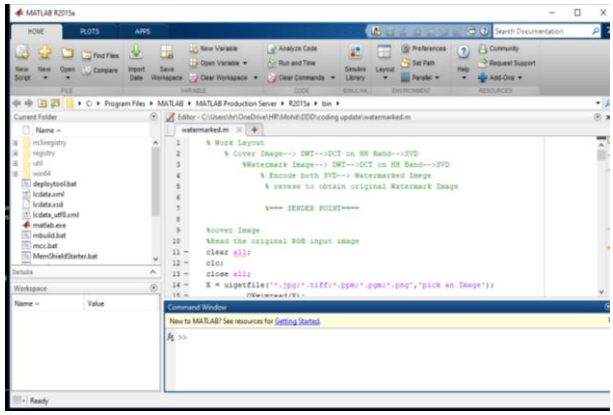

Fig. 5 Snapshot 1.

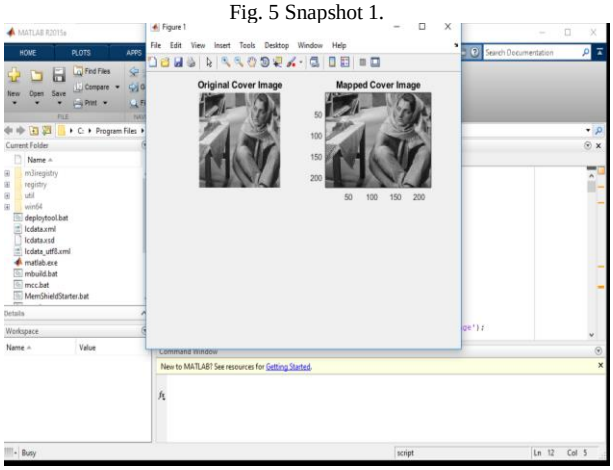

Fig. 6 Snapshot 2.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

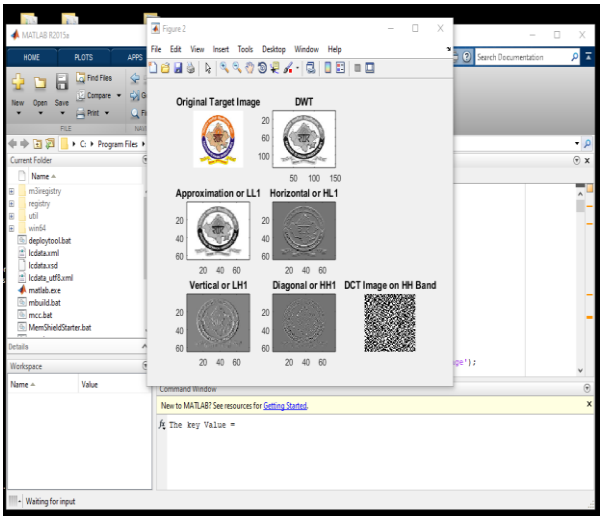

Fig. 7 Snapshot 3.

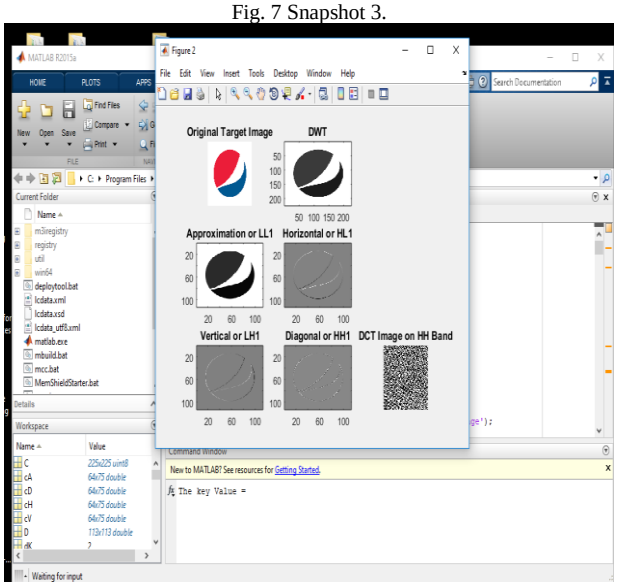

Fig. 8 Snapshot 4.

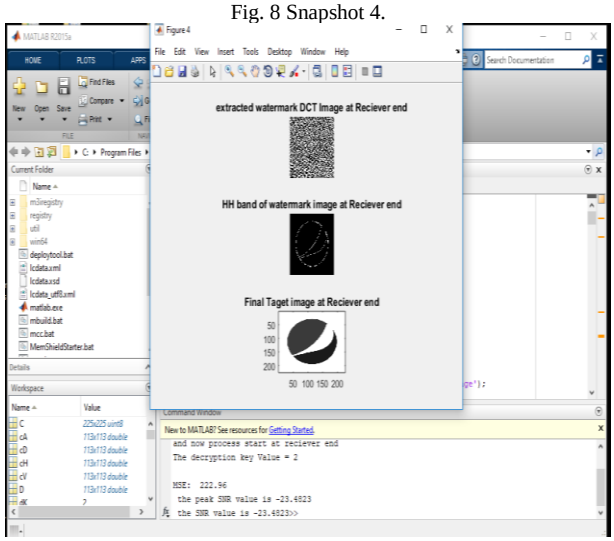

Fig. 9 Snapshot 5.

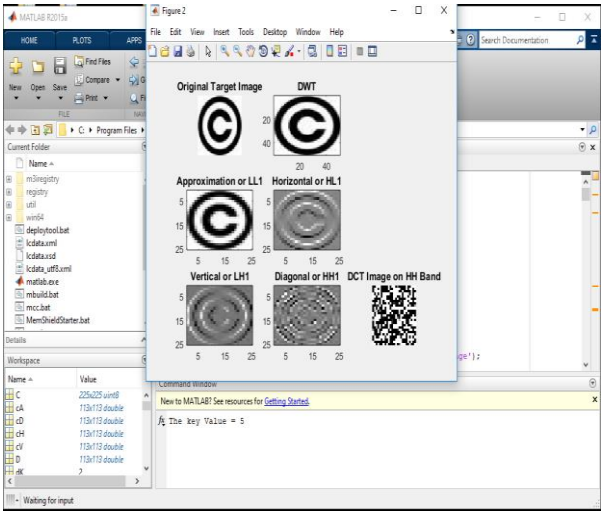

Fig. 10 Snapshot 6.

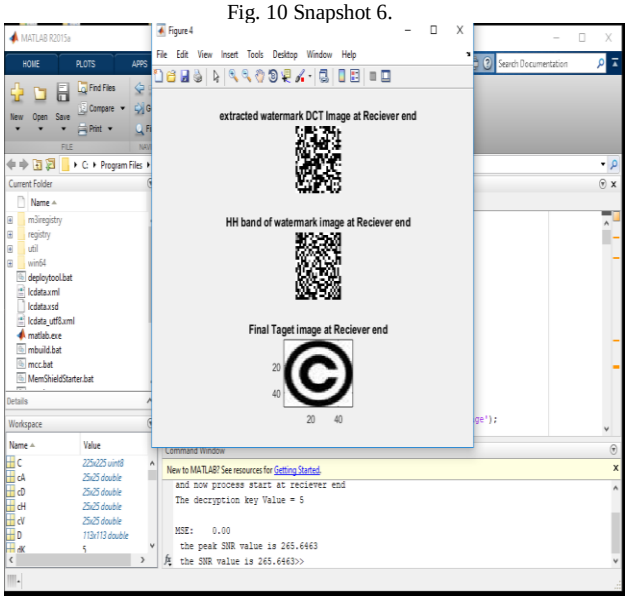

Fig. 11 Snapshot 7.

VII. CONCLUSION

During the research work the design that utilized DWT, DCT and SVD as cross breed watermarking and AES encryption to keep up and upgrade the security level of the general proposed approach. DWT is a standout amongst the most prominent watermark conspires so in this work we use DWT and for increment the presentation we additionally use DCT and SVD as half breed watermarking procedure and encryption calculation to improve the security parameter. Advanced Encryption standard calculation (AES) utilized for encoding the given transmission of information and a picture. Advanced Encryption Standard (AES) is an extremely ground-breaking standard square figure calculation contrasted with the information encryption standard (DES) algorithm. The proposed model can be further extensive to construct up a toolbar that has the all security instrument and approved client (beneficiary). During the proposed methodology we upgraded the security perspective yet increment the computational overhead. Along these lines, in upcoming period we limit the computational overhead with no impact on safety circumstances.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

REFERENCES

[1] P. Karthigaikumar, Soumiya Rasheed, "Simulation of Image Encryption using AES Algorithm", *IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE*, 2011, pp.166-172.

[2] Samir Kumar Bandyopadhyay, TuhinUtsab Paul and AvishekRaychoudhury, "Invisible Digital Watermarking Through Encryption", *International Journal of Computer Applications (0975 – 8887)*, Vol. 4, No.8, August 2010, pp.18-20.

[3] Navas K. A., Ajay Mathews Cheriyan, Lakshmi. M, Archana Tampy. S, and Sasikumar M, "DWT-DCT-SVD Based Watermarking", *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops*, pp. 271-274, 2008.

[4] F. Huang and ZH. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR", *Pattern Recognition Letters*, vol.25, pp.1769-1775, 2004.

[5] Radouane, M., "Robust method of digital image watermarking using SVD transform on DWT coefficients with optimal block", April 2014.

[6] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankarbabu, "Image Encryption Based on AES Key Expansion", *2011 Second International Conference on Emerging Applications of Information Technology*, IEEE, 2011, pp.217- 220.

[7] V. Amutha, C.T. Vijay Nagaraj, "A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm", *International Journal of Innovative Research in Science*, Engineering and Technology Volume 3, Special Issue 3, March 2014, pp. 1099-1104.

[8] Mohammad Ibrahim Khan, Md. Maklachur Rahmanand Md. Iqbal Hasan Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation", *Department of Computer Science and Engineering, Chittagong University of Engineering and Technology Chittagong*-4349, Bangladesh.

[9] P. Parashar, "A Survey: Watermarking Techniques", 2014.

[10] V. Gupta , "A Review on Image Watermarking and Its Techniques", *IJMEIT* ,Vol. 2, Issue 1, January 2014.

[11] P. Rahmati, A. Adler, and T. Tran, "Watermarking in E-commerce", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 6, 2013.