



Image Authentication Technique Based on Digital Watermarking using Clustering

Ridhima Sharma
Department of Computer Science & IT
University of Jammu
Jammu, India
ridhima.363@gmail.com

Jasbir Singh
Department of Computer Science & IT
University of Jammu
Jammu, India
jasbirmca@gmail.com

Abstract: The digital images are being widely used in computer applications. These can be modified without any limit by using different image processing software. As a result the concerned person can suffer from financial and public damage. To overcome this, a reliable digital image authentication scheme is required to be developed. Digital watermarking can be used as a solution to this problem. It is an efficient way to guarantee authenticity and integrity of digital images. A watermark is embedded in to the digital image which uniquely identifies the ownership and provides the security to it and can be easily extracted. In this paper, an image authentication scheme based on digital watermarking using clustering is proposed. We have used a combination of DCT and clustering together with image scrambling technique. DCT is used for watermark embedding process and Fuzzy C-Means is used for clustering. In order to improve the security of the proposed Digital Watermarking scheme, Arnold Transform is used that scrambles watermark before embedding it in to the cover image. Performance of the proposed work is evaluated based on Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC).

Keywords: Digital watermarking, Discrete Cosine Transform (DCT), Arnold Transform, Fuzzy C-Means Clustering, PSNR, MSE, NC

I. INTRODUCTION

The capture, transmission and storage of digital data have become very easy and convenient due to the success of the internet. In the last few years, more and more digital data is being distributed to a continuously growing number of people for sharing, studying and other purposes as a result of the fast development of digital multimedia and internet techniques. The digital data can be text, audio, video and software which are being transferred over the internet. Sharing data digitally is highly desirable because of its speed and cost efficiency. But most of the digital data is not protected. This can lead to the easy transferring, copying and tampering of the digital data. So the protection of digital data is desirable. Due to the increasing use of internet, the copyright protection and authentication of the digital data has become a significant issue. A popular resolution to the strong need of copyright protection and authentication of digital multimedia is Digital watermarking.

In this paper, a clustering based digital watermarking scheme is proposed. The watermark is first scrambled using Arnold Transform to enhance the security. The organization of the paper is as follows: Section 2 is about Digital Watermarking. Section 3 contains the related work. Section 4 describes the techniques used. The proposed method is provided in Section 5. Section 6 contains the Experimental analysis and results. Conclusion is given in Section 7.

II. DIGITAL WATERMARKING

Digital watermarking is the process of embedding a watermark in to the digital data. In it, information data, pattern, logos or labels can be embedded in to the digital multimedia. The watermark can be of text, audio image or video type.

A. Digital Watermarking Principle

Digital watermarking consists of two processes:
1. Watermark embedding: It is the process of embedding watermark in to the digital data [19].

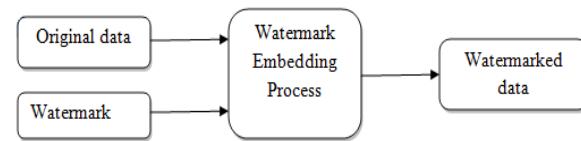


Figure 1. Watermark Embedding [19].

2. Watermark extracting: It is the process of extracting embedded watermark from the watermarked data [19].

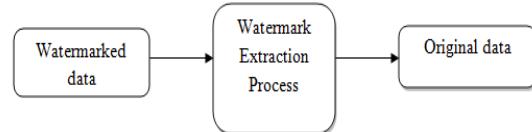


Figure 2. Watermark Extracting [19].

B. Clustering for Digital Watermarking

Clustering is an unsupervised learning method. It is the process of organizing the objects in to clusters such that the objects in the same cluster are as similar as possible and the objects in different cluster are as different as possible [22]. The construction of clustering algorithms are based on distance (or dissimilarity) and similarity [22]. Distance function is used to determine the relationship among the quantitative data while similarity function is used for the qualitative data. Different sets of useful data can be obtained by applying clustering on images [7].

Image clustering simplifies the representation of an image and makes its analysis easier. An image is first divided into various segments which are then combined according to some rules. The aim is to form clusters which have same characteristics.

III. RELATED WORK

The process of embedding the watermark in to the digital data is called Digital Watermarking. The method of embedding

the watermark can be either spatial domain or frequency (transform) domain.

In spatial domain based watermarking, the watermark is embedded directly by modifying the gray values of pixels of cover image.

Sanjay Kumar et al. [12] compared two spatial domain digital watermarking schemes. In the first watermarking scheme the watermark is embedded in to the cover image based on LSB substitution. While in the second algorithm, the cover image is divided into different blocks and for each block the entropy value is calculated. The selected watermark is embedded in to the maximum entropy value block using the LSB substitution technique. MSE and The comparison result shows that the algorithm based on entropy is better as compared to the watermarking algorithm based on LSB substitution. The first algorithm is more robust to Gaussian noise than the second algorithm.

Abdullah Bamatraf et al. [23] proposed a Least Significant Bits technique for digital watermarking based on the use of 3rd and 4th least significant bits. This watermarking scheme is robust and simple. It works better as compared to the traditional LSB technique which is based on the use of 1st least significant bit for hiding the data.

In transform domain watermarking, the watermark is embedded in to the coefficients of host data transform. The most commonly used transform techniques are: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT).

C. Thirumurai Selvi et al. in [1] proposed a DWT based watermarking approach for authentication of medical images. The details of the patients are concealed in the medical images as a watermark. The DWT is applied to the input/cover image which divides it in to 3 high frequency sub bands LH (Low-High), HL (High-Low), HH (High-High) and 1 low frequency band LL (Low-Low) and the watermark is embedded in to the LL sub band of the cover image. Deepati Agrawal et al. [8] proposed a discrete cosine transform (DCT) and image segmentation based watermarking scheme. First the image is segmented. Each segment is then divided in to 8x8 pixel blocks. The blocks are reordered using the zigzag reordering algorithm. A 2D DCT is applied for each 8x8 block. The watermark is embedded in to the DCT coefficients of each segment. The proposed scheme is highly robust against various attacks.

Ravi K Sheth et al. [9] proposed a secure digital image watermarking. A combination of DCT, DWT and cryptographic method is used to obtain an efficient and secure scheme. DCT is first applied to the original image and Arnold transform is used to encrypt the message image. In the second step DWT is applied to the cover image and DCT is performed on the message image. The DWT coefficients of LL band are modified and secrete message is embedded in to it. The proposed scheme is highly robust against various attacks.

Table 1 provides summary of various spatial and transform domain watermarking techniques.

Table I. Summary Of Spatial And Transform Domain Watermarking Techniques

Author	Methodology	Spatial Domain	Frequency Domain
C. T. Selvi et al.[1]	proposed a DWT based watermarking approach for authentication of medical images.	✗	✓
D. Agrawal et al. [8]	proposed a discrete cosine transform (DCT) and image segmentation based watermarking scheme.	✗	✓
R. K. Sheth et al. [9]	A combination of DCT, DWT and cryptographic method is used to obtain an efficient and secure digital image watermarking.	✗	✓
M. Srivastava et al. [11]	proposed a watermarking scheme based on Triple DES and spatial domain.	✓	✗
S. Kumar et al. [12]	compared two spatial domain digital watermarking schemes.	✓	✗
Y. Yang et al. [13]	implemented DCT algorithm for Digital Watermarking on MATLAB.	✗	✓
N. Bansal et al. [14]	compared 3 digital watermarking schemes, that is, LSB technique, DWT transform and DCT transform.	✓	✓
K. Raval et al. [16]	proposed a DCT-DWT based digital watermarking algorithm.	✗	✓
A. Upadhyay et al. [18]	proposed a color image watermarking scheme for telemedicine application which is imperceptible and robust.	✗	✓
A. Bamatraf et al. [23]	proposed a Least Significant Bits (LSB) technique for digital watermarking based on the use of 3 rd and 4 th least significant bits.	✓	✗
N. SenthilKumaran et al. [24]	provides the comparison analysis of DWT based watermarking scheme and LSB based watermarking.	✓	✓
Xiao-Long Liu et al. [25]	proposed a blind watermarking scheme that can be used for both copyright protection and authentication of the color images.	✓	✓

Clustering algorithms can be used for steganography and digital watermarking applications. Bhagya Pillai et al. in [7] proposed an image steganography method based on encryption techniques and k-means clustering. In the proposed approach, the secret message is first encrypted using DES. After this, k-

means clustering is used to obtain k segments of the cover image. The k segments of encrypted message are obtained which is followed by hiding the message segments in to cover image clusters. The use of clustering and cryptographic techniques together in steganography provides better security.

Balpreet Kaur et al. [17] proposed an improved technique for color image segmentation based on Fuzzy C-Means clustering. The existing threshold based methods perform fine for images that contain only two components. FCM is a grouping technique which is unsupervised. Rather than belonging completely to just one cluster, each point has a degree of belonging to clusters.

Table 2 provides summary of various clustering based watermarking & steganography techniques.

Table II. Summary of Clustering Based Watermarking & Steganography Techniques

Author	Methodology	Clustering Algorithm
Bhagya Pillai et al.[7]	proposed a image steganography method based on encryption techniques and k-means clustering.	K-means
Manickam.L et al.[2]	presented a scheme for tamper detection and image authentication based on k-means clustering.	k-means
Rohit Singh et al.[4]	proposed fuzzy mean clustering approach for digital watermarking.	fuzzy mean clustering
Mohamed Tahar et al [3]	proposed a new clustering technique known as Content Addressable Method(CAM) for digital watermarking.	CAM clustering
R. Suganya [5]	presented a scheme for tamper detection and image authentication based on k-means clustering for bio medical images.	k-means
Dharamvir [6]	proposed a Fuzzy C means (FCM) clustering for image authentication	FCM
A.SaiKrishna et al. [15]	proposed a method that makes use of k-means clustering algorithm along with LSB substitution technique for steganography.	k-means

Cryptography and digital watermarking can be used together for improved security. Ali Al-Haj et al. [10] proposed a scheme for transmitting medical images using both watermarking and cryptography. In the proposed scheme, a cover image is used to hide the data of the patient. Firstly, the ROI and RONI regions of the medical image are separated. The watermark is embeded in the RONI region. The watermarked image is obtained by combining the ROI and watermarked RONI region.

Mudita Srivastava et al. [11] proposed a watermarking scheme based on Triple DES and spatial domain. In order to

obtain higher level of privacy and efficiency, cryptography and digital watermarking are used together. The watermark is encrypted by using Triple DES algorithm and then it is embedded in the spatial domain of the cover image to obtain a watermarked image. As a result of this it becomes almost impossible for an intruder to remove or modify message from the spatial domain of the cover image.

IV. TECHNIQUES USED

A. Arnold Transform

The communication of digital images safely is extremely important because of the fast development of internet and multimedia. Digital watermarking is one way to provide protection to the digital images. An important image encryption scheme known as Image Scrambling can be used along with Digital Watermarking to provide more security. Image Scrambling is the process of making the spatial positions of the pixels chaotic so that the original meaning of the image is lost and it becomes hard to identify [31].

Arnold transform is an Image Scrambling technique. It is widely used with Digital Watermarking as it has the characteristic of periodicity and simplicity [32]. The periodicity of Arnold Scrambling means that it is possible to restore the original image after several cycles [32]. It is applicable to the square images only [33].

Digital image consists of image points called pixels. It is represented by a two-dimensional function $F(x, y)$, where x & y are the coordinates and F is the gray level [33]. In Arnold Transform, the pixel positions are shifted from (x, y) to (x', y') . A disordered image is generated after several transformations. After a certain number of iterations, the original image can be recovered, making the process cyclic and reversible [31].

Arnold Transform is given by the following equation [34]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) \quad (1)$$

Inverse Arnold Transform is given by the equation [33]:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (\text{mod } N) \quad (2)$$

Where (x, y) = original image pixel coordinates.

(x', y') = scrambled image pixel coordinates.

N = height or width of the original image.

The period of Arnold Scrambling is the time after which the shuffled image is restored back to the original image [35]. It depends on the image dimensions, that is, height or width ($N \times N$) of the image that is required to go through the process. This technique causes the image iterations to occur [34]. If the image is iterated for k iterations to obtain the chaotic/messy image, k becomes the secret key that is used to encrypt and extract the secret image [31, 34]. An attacker will require this key to get the original meaningful watermark [34].

The period of Arnold Transform (τ) can be given by the following equations [49, 50]:

$$\tau = 3n \text{ if and only if } n = 2 \cdot 5^k \quad k = 1, 2, \dots$$

$$\tau = 2n \text{ if and only if } n = 5^k \text{ or } 6 \cdot 5^k \quad k = 1, 2, \dots$$

$$\tau = \frac{12n}{7} \text{ for all other choices of } n.$$

Table 3 shows different Arnold Transform Periodicities.

Table III. Arnold Transform Periodicities

N	7	64	120	124	125	128	256	480	512
T	8	48	60	15	250	96	192	120	384

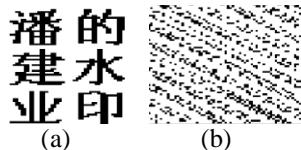


Figure 3. (a) Original Image (b) Image after Arnold transform

Consider a pixel $\begin{bmatrix} 4 \\ 6 \end{bmatrix}$ of a 7×7 Image. It follows the below path:

$$\begin{aligned} T \begin{bmatrix} 4 \\ 6 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 4 \\ 6 \end{bmatrix} \pmod{7} = \begin{bmatrix} 4+6 \\ 4+12 \end{bmatrix} \pmod{7} = \begin{bmatrix} 10 \\ 16 \end{bmatrix} \\ (\text{mod } 7) &= \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow \begin{bmatrix} 5 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 5 \\ 5 \end{bmatrix} \rightarrow \begin{bmatrix} 3 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 5 \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 6 \end{bmatrix} \end{aligned}$$

After 8 iterations, a 7×7 Arnold Scrambled Image is restored to its original form. Thus, a 7×7 image has a period of eight.

B. Discrete Cosine Transform (DCT)

A popular frequency domain watermarking scheme is Discrete Cosine Transform (DCT). It uses a cosine waveform to convert a signal from the spatial domain to the transform domain [16]. The various fields in which Discrete Cosine Transform is useful are: compression, pattern recognitions, digital image processing etc [34].

When applied to an image, Discrete Cosine Transform divides it into different frequency bands: low-frequency (F_{LOW}), mid-frequency (F_{MID}) and high-frequency (F_{HIGH}) [39, 48]. The watermark can be embedded into one of these bands. The low-frequency (F_{LOW}) band contains the important and visible areas of the image. It is sensitive (vulnerable) to Human Visual System [36]. Any changes implemented in this band can be easily detected by the human eye [27]. On the other hand the application of attacks, such as noise and compression, can lead to the elimination of high frequency regions of the image [34, 36]. The mid-frequency band is considered to be the best region for embedding the watermark [16, 27, 34, 36]. The observable quality of the image is not altered or influenced when the watermark is inserted in to the mid-frequency band.

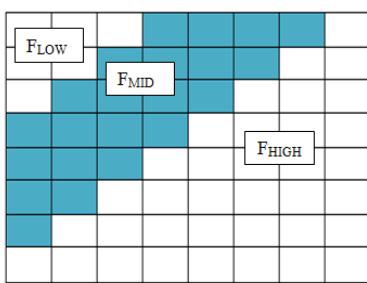


Figure 4. DCT Frequency Band [39].

The robustness of Discrete Cosine Transform based digital watermarking schemes is greater as compared to spatial domain watermarking schemes [20]. It is a faster technique having the complexity equal to $O(n \log n)$ [27].

Neha Bansal et al. [14] compared 3 digital watermarking schemes (LSB technique, DWT transform and DCT transform) using PSNR (Peak Signal-to-Noise Ratio) & NC (Normalized Correlation) and concluded that DCT is the best technique to be used for digital watermarking.

Discrete Cosine Transform based watermarking schemes are resilient against straightforward image processing operations like blurring, adjustment of contrast & brightness, low pas

filtering etc [38]. But are not strong against geometric transformations like: scaling, cropping, rotation etc [38]. The computational complexity of DCT algorithms is less as compared to the DWT based watermarking techniques [38]. The various advantages of DCT are [13, 39]:

1. The computational complexity is less
2. High compression ratio.
3. The error rate is low. It is defined as the ratio between the number of bit errors and the total bits transferred during a time interval. There is a small error between the original and reconstructed signal.
4. It provides a good concealing.

The Discrete Cosine Transform is appropriate for watermarking because of its high energy compaction and the easy availability of fast algorithms for the calculation of transform [39]. The energy compaction characteristic of DCT allows concentrating the data into as few coefficients as possible [37].

C. Fuzzy C-Mean Clustering

There are two types of clustering: Hard Clustering & Fuzzy Clustering [40]. In hard clustering, each data element can belong to only one cluster [40]. It is also known as classical crisp clustering. In fuzzy clustering, a data element can belong to more than one cluster [40]. The degree to which individual data elements belong to a cluster is expressed by a membership value associated with it [41]. The membership value can be between 0 and 1 [40, 41]. A gradual membership is allowed in FCM [4]. As compared to other clustering algorithms, FCM is faster as it uses degree of membership of a data element to a given cluster, instead of using the absolute membership [17].

In FCM, the selection of the clusters is based on the mean (centroid) of all the given data elements. The data elements are first divided in to two clusters, that is, above and below the mean. The data element that exactly matches the mean value belongs to both the cluster. The mean of both the clusters is computed again and the clusters are further divided in to sub clusters [4]. This process continues until the centroids do not change. A membership value is given to each data element based on the distance between the data point and the cluster center [41]. The membership value of a data point is higher if it is near to the center of the cluster [17, 41].

The advantages of Fuzzy C-Mean Clustering are:

1. The Fuzzy C-Mean Clustering algorithm is faster as compared to other clustering algorithms [17].
2. It provides better result for overlapped data [42].

When an image contains well-defined structure, such as regular shapes and edges, hard clustering is effective. But in the presence of ill-defined data, it does not perform very well. Fuzzy regions are produced when such images are processed. The fuzzy clustering provides best result for such imprecise data [43].

V. PROPOSED METHOD

A. Introduction

The transmission and storage of digital images have become easy due to the development of internet. There are a number of image processing software systems that can be used to tamper with these images. So, the authentication of digital

images has become a necessity. Digital watermarking can be used as a solution to this problem.

The purpose of this research work is to provide a method for image authentication based on digital watermarking using clustering. It specifically focuses on the digital image watermarking.

B. Proposed Work

Digital Image Watermarking Method using Discrete Cosine Transform and Clustering is proposed. Fig. 5 presents a general block diagram for the proposed approach. The different techniques that are utilized are:

1. Arnold Transform: It is an image scrambling technique. It is used to encrypt the input watermark image. This is done to enhance the security of the proposed watermarking approach.
2. Discrete Cosine Transform: The cover image is converted from spatial domain to the frequency domain using DCT.
3. Fuzzy c-mean clustering: It is used to divide the cover image in to various clusters. Image clustering simplifies the representation of an image and makes its analysis easier.

We have divided our proposed work in to three phases as shown in Fig. 5. These are:

Phase-1: In it, the original watermark image is scrambled using Arnold Transform to obtain an encrypted watermark. Phase-1 is further divided in to three sub modules: Original Watermark, Arnold Transform and Encrypted Watermark.

Phase-2: In it, the encrypted watermark from Phase-1 is inserted in to the cover image using DCT and Fuzzy c-means clustering approaches to obtain the watermarked image. This phase consists of 3 sub modules: Cover Image, Watermark Embedding and Watermarked Image

The purpose of this research work is to provide a method for image authentication based on digital watermarking using clustering. It specifically focuses on the digital image watermarking.

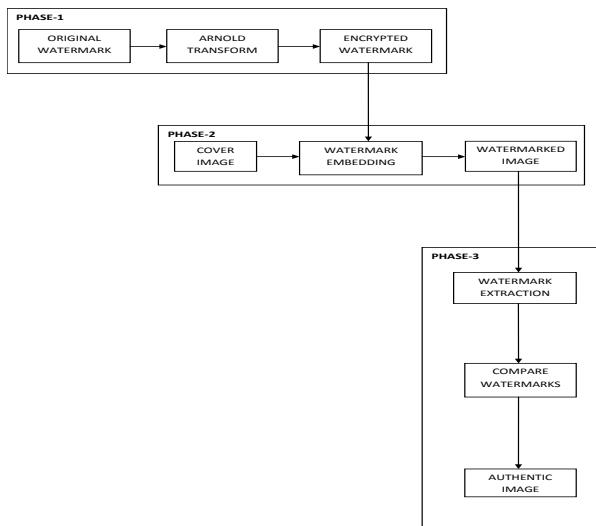


Figure 5. A general Block Diagram of the proposed approach.

Phase-3: In it, the watermark is extracted from the watermarked image (from Phase-2). The extracted watermark is compared to the original watermark. If the two watermarks are similar, then the cover image generated during the watermark extraction process is considered to be authentic.

The detailed description of watermark embedding and watermark extraction procedures is provided in section C and D respectively.

C. Watermark Embedding

The process of embedding the watermark in to the cover image consists of the following steps:

1. The cover image (as in Phase-2) and the watermark image (as in Phase-1) are first taken as an input from the user. An image watermark is being used instead of the text watermark. It is because of the fact that if there is a mistake of one symbol in case of text watermark, the entire watermarking scheme can fail. On the other hand, image watermarks can tolerate some distortions. Also images can be better understood by the Human Visual System (HVS).
2. The watermark image is then encrypted using the Arnold Transform (as in Phase-1). It is an Image Scrambling technique that changes the image pixel positions to generate a non-recognizable image.
3. The cover image (as in Phase-2) is converted from the spatial domain to the transform domain using Discrete Cosine Transform (DCT). The cover image is first divided in to 8x8 blocks. DCT is applied to each block. It divides each 8x8 block of the cover image into three different frequency bands: low-frequency, mid-frequency and high-frequency.
4. Fuzzy C-Means Clustering is applied on the cover image to form four clusters. Alpha blending technique [45, 46] is used for embedding the watermark in to the clusters.
5. Inverse DCT (IDCT) is applied on each block to obtain the Watermarked Image (as in Phase-2).

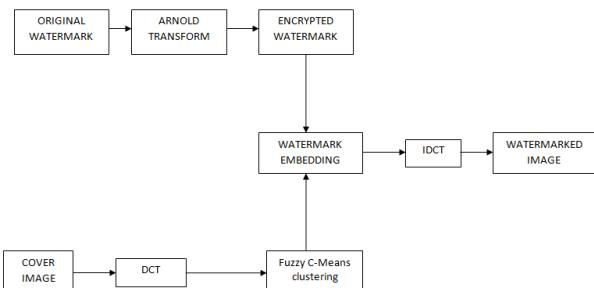


Figure 6. Block Diagram for Watermark Embedding Process

D. Watermark Extraction

The process of extracting the watermark from the watermarked image includes the following steps:

1. Apply 8X8 2D-DCT on the watermarked image to convert it from spatial domain to transform domain.
2. Fuzzy C-means clustering is again applied to form four clusters. The watermark is then extracted from the clusters using the alpha blending technique.
3. Apply inverse Arnold Transform to the extracted watermark.
4. Compare the recovered watermark and the original watermark using Normalized Correlation (NC). If the two watermarks are same, then obtained image is authentic.

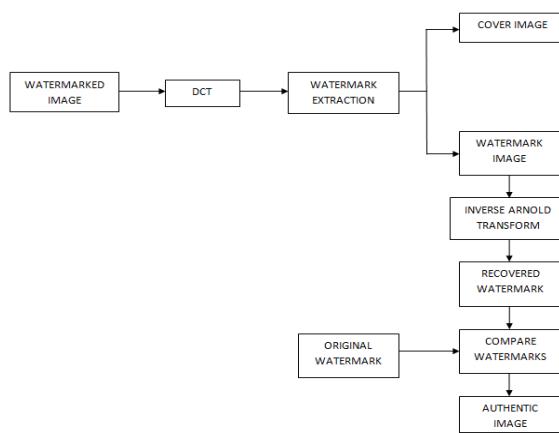


Figure 7. Block Diagram for Watermark Extraction Process.

E. Experimental Framework

The experimental framework of the proposed Digital watermarking approach is shown in Fig. 8:

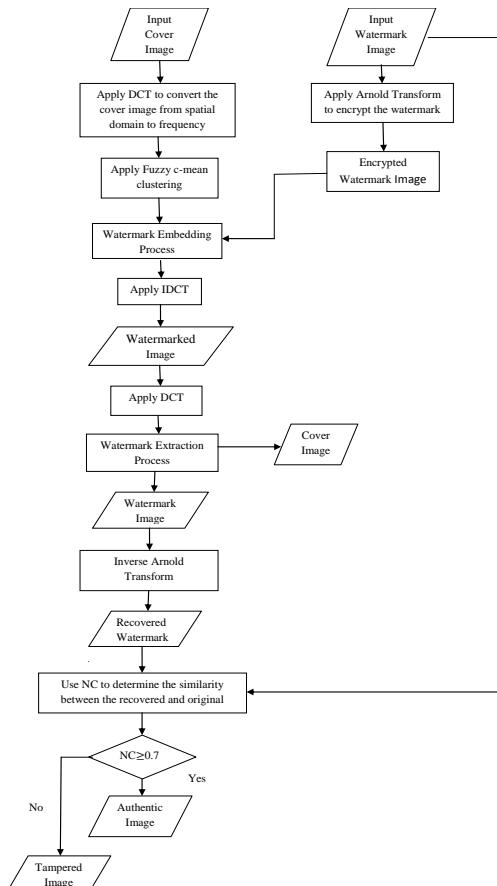


Figure 8. Experimental Framework.

VI. EXPERIMENTAL ANALYSIS AND RESULTS

A. Tool Used

The proposed Digital Watermarking approach is implemented in MATLAB version R2013a.

B. Images Used

Four grayscale images of size 256x256 are used as cover images shown in Fig. 9. Two grayscale images of size 64x64 are used as watermark images shown in Fig. 10. The embedding of the watermark in to the cover image is done by

the proposed DCT and Clustering based watermarking scheme. Arnold Transform is used to scramble the watermark images.

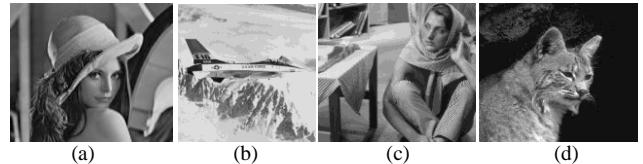


Figure 9. (a) lena (b) airplane (c) Barbara (d) cat.

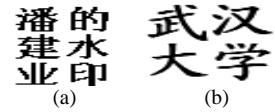


Figure 10. (a) watermark1 (b) watermark2.

C. Performance Evaluation

Consider as an example, Lena as input cover image and watermark1 as input watermark. Fig. 11(a) shows the embedding of watermark1 in to the cover image Lena to obtain a watermarked image. The watermark image is scrambled using Arnold Transform. Fig. 11(b) shows the extracting of watermark1 from the cover image Lena.



Figure 11. (a) Output of the Watermark Embedding Process in MATLAB
(b) Output of the Watermark Extracting Process in MATLAB

The performance of the proposed watermarking approach is determined by using two parameters: Peak Signal-to-Noise

Peak Signal to Noise Ratio:

PSNR is used to measure the similarity between the watermarked image and original image, that is, imperceptibility of watermarked image [27]. The PSNR value is calculated in decibels (dB) [26]. Higher the value of PSNR, the better the quality of the watermarked image [27]. The PSNR value above 30dB indicates acceptable quality of the image [28].

The PSNR value can be calculated using the following equation [44]:

$$\text{PSNR} = 10 \log_{10} (\max I^2 / \text{MSE}) \quad (3)$$

$\max I$ = maximum possible pixel value of the image.

Mean Squared Error (MSE) is the simplest parameter to determine the similarity between the watermarked image and the original image. The cumulative squared error between the watermarked image and the original image is represented by MSE [26]. The lower value of MSE indicates better quality of the image.

The equation to calculate MSE:

$$\text{MSE} = \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N \{X(i, j) - X_w(i, j)\}^2 \quad (4)$$

$X(i, j)$ = original image pixel value.

$X_w(i, j)$ = watermarked image pixel value.

Normalized Correlation

Normalized Correlation is used to determine the similarity between the extracted watermark and the original watermark [27]. It can also be used to measure the similarity between the watermarked image and the original image [27]. Higher the

value of NC, the better the quality of the watermarked image [27]. The value of Normalized Cross-Correlation is between 0-1 [29]. The two images are same if NC=1 and different if NC=0. The NC value 0.7 or above is considered to be acceptable [30].

NC can be calculated by using the formula [29, 30]:

$$NC = \frac{\sum_i \sum_j I(i,j) I_w(i,j)}{\sqrt{\sum_i \sum_j [I(i,j)]^2} \sqrt{\sum_i \sum_j [I_w(i,j)]^2}} \quad (5)$$

$I(i, j)$ = original image pixel value; $I_w(i, j)$ = watermarked image pixel v.

Table 4 shows PSNR values obtained for different cover images.

Table IV. PSNR Values Of Different Cover Images Using Proposed Model

Cover Image	Watermark Image	Watermarked Image	PSNR
lena	watermark1 		49.8940
lena	watermark2 		49.8613
airplane	watermark1 		49.8940
airplane	watermark2 		49.8613
barbara	watermark1 		49.8940
barbara	watermark2 		49.8613
cat	watermark1 		49.8940
cat	watermark2 		49.8613

The various watermarked images obtained by using the proposed method are also shown in Table 4. It can be seen that the cover image and the watermarked image are perceptually similar for every combination of cover image and watermark image.

Table 5 shows NC values obtained by comparison between the original watermark and extracted watermark for the proposed model.

Table V. NC values for comparison between the original watermark and extracted watermark

Cover Image	Watermark Image	Watermarked Image	Extracted Watermark	NC
lena	watermark1 			0.9954
lena	watermark2 			0.9982
airplane	watermark1 			0.9954
airplane	watermark2 			0.9982
barbara	watermark1 			0.9954
barbara	watermark2 			0.9982
cat	watermark1 			0.9954
cat	watermark2 			0.9982

VII. CONCLUSION

Digital Image Watermarking is the process of embedding a watermark into the cover image. It can be used to provide authentication to the extensively used digital images.

In the research work, an image authentication scheme based on digital watermarking using clustering is proposed. The different techniques are used i.e. Discrete Cosine Transform (DCT), Fuzzy C-Mean Clustering and Arnold Transform. An image watermark is used instead of the text watermark. The security of the proposed scheme is improved by encrypting the watermark image using Arnold Transform. The parameter Peak

Signal-to-Noise Ratio (PSNR) is used to ascertain the performance of proposed watermarking scheme to ensure the quality of the watermarked image. For the proposed method, we get the average PSNR value for all used images greater than 30db i.e. 49.877. This indicates that differentiating between the cover image and watermarked image will be difficult. Hence, the quality of the watermarked image is acceptable. The authenticity of the image is determined by comparison between the extracted watermark and the original watermark. The parameter Normalized Correlation (NC) is used for this. The value of NC greater or equal to 0.7 indicates the image is authentic. In future, the proposed scheme will be extended for color images. Also, other techniques for encrypting watermark image will be taken into consideration.

VIII. REFERENCES

- [1] C.Thirumarari Selvi, R.Sudhakar , Priyadarshini.G, "DWT based watermarking approach for medical image authentication", *IEEE International conference on Intelligent Systems and Control (ISCO)*, DOI: 10.1109/ISCO.2016.7726895, January 2016.
- [2] Manickam.L, Dr S.A.K. Jilani, Dr.M.N.Giri Prasad, "A Novel Fragile Watermarking Scheme For Image Tamper Detection Using K Mean Clustering", *International Journal of Computer Trends and Technology (IJCTT)*, volume 4, Issue10, pp.3380-3385, Oct 2013.
- [3] Mohamed Tahar Ben Othman, "Digital Image Watermarking based on image clustering", *3rd International Conference on Circuits, Systems, Communications, Computers and Applications (CSCCA '14)*, November 2014.
- [4] Rohit Singh, Pancholi Bhavna K, "A Noble Technique for Digital Image Watermarking Authentication Using Fuzzy Mean Clustering", *International Journal of Science and Research (IJSR)*, pp. 207–209, DOI: 10.21275/v5i4.nov162449.
- [5] R. Suganya and Dr. R Kanagavalli, "Tamper Detection using Watermarking Scheme and K-Mean Clustering for Bio Medical Images", *International Journal for Modern Trends in Science and Technology*, Volume:02, Issue No: 11, pp. 180-185, November 2016.
- [6] Dharamvir, "A Simple Approach on Image Authentication Watermarking", *International Journal of Computer Applications*, Volume 67– No.11, pp. 19-22, April 2013.
- [7] Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram, "Image Steganography Method Using K-Means Clustering and Encryption Techniques", *IEEE International conference on Advances in Computing, Communications and Informatics (ICACCI)*, DOI: 10.1109/ICACCI.2016.7732209, September 2016.
- [8] Deepati Agrawal, Vikas Gupta, Gaurav Mehta, "Digital Watermarking Technique using Discrete Cosine Transform", *International Journal of Engineering Innovation & Research*, Volume 2, Issue 1, pp. 9-12, 2013.
- [9] Ravi K Sheth and V.V Nath, "Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method", *2016 International Conference on Advances in Computing, Communication, & Automation*, pp. 1-5, DOI: 10.1109/ICACCA.2016.7578861, April 2016.
- [10] Ali Al-Haj, Noor Hussein and Gheith Abandah, "Combining cryptography and digital watermarking for secured transmission of medical images", *2016 2nd International Conference on Information Management (ICIM)*, pp. 40-60, DOI: 10.1109/INFOMAN.2016.7477531, May 2016.
- [11] Mudita Srivastava, H M Singh, Manish Gupta and Dharm Raj, "Digital watermarking using spatial domain and triple DES," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 3031-3035, March 2016.
- [12] Sanjay Kumar and Ambar Dutta, "Performance analysis of spatial domain digital watermarking techniques," *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1-4, DOI: 10.1109/ICICES.2016.7518910, Feb 2016.
- [13] Ying Yang and Haiping Li, "The application of DCT algorithm in digital watermarking by Matlab and simulation", *2015 7th International Conference on Modelling, Identification and Control (ICMIC)*, Sousse, pp. 1-5, DOI: 10.1109/ICMIC.2015.7409350, 2015.
- [14] N. Bansal, V. K. Deolia, A. Bansal and P. Pathak, "Comparative analysis of LSB, DCT and DWT for Digital Watermarking", *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, pp. 40-45, 2015.
- [15] A. SaiKrishna, S. Parimi, G. Manikandan and N. Sairam, "A clustering based steganographic approach for secure data communication", *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, Nagercoil, pp. 1-5, DOI: 10.1109/ICCPCT.2015.7159515, March 2015.
- [16] Keta Raval and Sameena Zafar, "Digital Watermarking with copyright authentication for image communication", *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, Gujarat, pp. 111-116, DOI: 10.1109/ISSP.2013.6526885, March 2015.
- [17] B. Kaur and P. Kaur, "Improving the color image segmentation using fuzzy-C-means," *2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, Ramanathapuram, pp. 789-794, DOI: 10.1109/ICACCCT.2016.7831747, May 2016.
- [18] A. Upadhyay and M. Dave, "Robust and imperceptible color image watermarking for telemedicine applications," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 1104-1109, DOI: 10.1109/ICCCA.2016.7813881, April 2016.
- [19] Ruchika Patel and Parth Bhatt, "A Review Paper on Digital Watermarking and its Techniques", *International Journal of Computer Application*, Volume 110-No. 1, pp. 10-13, January 2015.
- [20] Manjeet Kaur, Seema Baghla and Sunil Kumar, "A Review On Watermarking Of Digital Images", *International Journal of Advances in Science Engineering and Technology*, Volume- 3, Issue-3, pp. 149-153, July-2015.
- [21] Hussain Nyeem, Wageeh Boles and Colin Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks" *EURASIP Journal on Advances in Signal Processing*, pp. 1-22, DOI: 10.1186/1687-6180-2014-135, 2014.
- [22] Dongkuan Xu and Yingjie Tian, "A Comprehensive Survey of Clustering Algorithms", *Annals of Data Science*, Volume 2, Issue 2, pp. 165-193, DOI: 10.1007/s40745-015-0040-1, June 2015.
- [23] Abdullah Bamatraf, R. Ibrahim and M. N. B. M. Salleh, "Digital watermarking algorithm using LSB", *2010 International Conference on Computer Applications and Industrial Electronics*, Kuala Lumpur, pp. 155-159, DOI: 10.1109/ICCAIE.2010.5735066, Dec 2010.
- [24] N. S. Kumaran and S. Abinaya, "Comparison analysis of digital image watermarking using DWT and LSB technique," *2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, pp. 0448-0451, doi: 10.1109/ICCSP.2016.7754176, April 2016.
- [25] X. L. Liu; C. C. Lin; S. M. Yuan, "Blind dual watermarking for color images authentication and copyright protection", *IEEE Transactions on Circuits and Systems for Video Technology*, Volume PP, Issue 99, pp.1-1, DOI: 10.1109/TCSVT.2016.2633878, Dec 2016.

- [26] S. Bhatt, A. Ray, A. Ghosh and A. Ray, "Image steganography and visible watermarking using LSB extraction technique", *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, pp. 1-6, DOI: 10.1109/ISCO.2015.7282315, Jan 2015.
- [27] Pooja Dabas and Kavita Khanna, "A Study on Spatial and Transform Domain Watermarking Techniques", *International Journal of Computer Applications*, Volume 71, Issue 14, May 2013.
- [28] Pradhan C., RathS. and Kumar Bisoi A. , "Non Blind Digital Watermarking Technique Using DWT and Cross Chaos", *2nd International conference on communication, computing, and security*, pp. 897-904, 2012.
- [29] Yusuf Perwej, Firoj Parwej and Asif Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", *The International Journal of Multimedia & Its Applications (IJMA)*, Volume 4, Issue 2, April 2012.
- [30] Iman M.G. Alwan and Enas Muzaffer Jamel, "Digital Image Watermarking Using Arnold Scrambling and Berkeley Wavelet Transform", *Al-Khwarizmi Engineering Journal*, Vol. 12, No. 2, pp. 124-133, 2016.
- [31] Sadik Ali Al-Tawee, Mohammed. Al-Hada, Ahmed. M. A. Naser, and Mohammed Al-Thamary, "Hide Image in Image Based on LSB Replacement and Arnold Transform", *7th International Conference on Information Technology (ICIT)*, pp. 319-323, DOI:10.15849/icit.2015.0048, 2015.
- [32] Min Li, Ting Liang and Yu-jie He, "Arnold Transform Based Image Scrambling Method", *3rd International Conference on Multimedia Technology (ICIT)*, pp. 1308-1316, DOI: 10.2991/icmt-13.2013.160, 2013.
- [33] Yugandhara H. Wankhede and Samadhan D. Mali, "Data Hiding Technique Using Audio Watermarking", *International Journal Of Engineering And Computer Science*, ISSN: 2319-7242, Volume 4, Issue 3, pp. 11109-11112, March 2015.
- [34] Majdi Farag Mohammed El Bireki, M. F. L. Abdullah, Ali Abdurhman M. Ukasha and Ali A. Elrowayati, "Digital Image Watermarking Based On Joint (DCT-DWT) and Arnold Transform", *International Journal of Security and Its Application*, Volume 10, Issue 5, pp. 107-118, 2016.
- [35] Siva Shankar S and A. Rengarajan, "Data Hiding in Encrypted Images using Arnold Transform", *ICTACT Journal On Image And Video Processing*, Volume 07, Issue 01, ISSN: 0976-9102, DOI: 10.21917/ijivp.2016.0194, August 2016.
- [36] Farhad Saeed, Mehdi Golestanian and Mohamadreza Azimi, "A Blind Watermarking Algorithm Based On DCT-DWT and ARNOLD Transform", *International Journal of Computer Science Engineering (IJCSE)*, ISSN: 2319-7323, Vol. 2, Issue 06, November 2013.
- [37] From <http://citeseerx.ist.psu.edu/viewdoc/citations?doi=10.1.1.18.4.6102>.
- [38] Aaqib Rashid, "Digital Watermarking Applications and Techniques: A Brief Review", *International Journal of Computer Applications Technology and Research*, Volume 5, Issue 3, pp. 147-150, ISSN: 2319-8656, 2016.
- [39] Harsh Vikram Singh, "Digital Image Watermarking Algorithm Based on DCT and Spread Spectrum", *UACEE International Journal of Advances in Electronics Engineering*, Volume 1, Issue 1, ISSN 2278 - 215X.
- [40] Anjana Gosain and Sonika Dahiya, "Performance Analysis of Various Fuzzy Clustering Algorithms: A Review", *7th International Conference on Communication, Computing and Virtualization (ICCCV)*, Volume 79, pp. 100-111, DOI: 10.1016/j.procs.2016.03.014, 2016.
- [41] Raulji Jitendrasinh G, "A Review on Fuzzy C-Mean Clustering Algorithm", *International Journal of Modern Trends in Engineering and Research (IJMTER)*, Volume 02, Issue 02, e-ISSN: 2349-9745, p-ISSN: 2393-8161, February 2015.
- [42] From <https://sites.google.com/site/dataclusteringalgorithms/fuzzy-c-means-clustering-algorithm>.
- [43] Gour Chandra Karmakar and Laurence Dooley, "A Generic Fuzzy Rule Based Technique For Image Segmentation", *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings*, pp. 1577-1580, volume 3, DOI: 10.1109/ICASSP.2001.941235, 2001.
- [44] Sonika C. Rathi, "Medical Image Authentication through Watermarking Preserving ROI", M.Tech. thesis, Department of Computer Engineering and Information Technology, College of Engineering, Pune, Maharashtra, June 2012.
- [45] P. Sharma and S. Swami "Digital Image Watermarking Using 3 level Discrete Wavelet Transform", *Conference on Advances in Communication and Control Systems (CAC2S)*, pp. 129-133, 2013.
- [46] Asha N, Bhagya P, "An Efficient Fingerprint Watermarking Approach Using 3 Levels DWT and Alpha Blending Technique", *Imperial Journal of Interdisciplinary Research (IJIR)*, Vol-2, Issue-13, 2016.