International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

Image Copy-Move Forgery Detection Using Key-Point Based Detection

Ms.P.R.Hemalatha, R.Kushmitha, R.Sruthy, V.Vaishali, V.Vaishnavi

Associate Professor, Dept. of C.S.E, Velammal College of Engineering and Technology, Madurai, India

UG Scholar, Dept. of C.S.E, Velammal College of Engineering and Technology, Madurai, India

UG Scholar, Dept. of C.S.E, Velammal College of Engineering and Technology, Madurai, India

UG Scholar, Dept. of C.S.E, Velammal College of Engineering and Technology, Madurai, India

UG Scholar, Dept. of C.S.E, Velammal College of Engineering and Technology, Madurai, India

ABSTRACT: Image forensic techniques is used to determine the integrity of images by applying various high-tech mechanisms. Image forensic techniques is used to determine the integrity of images by applying various high-tech mechanisms. Here, the images are analyzed for a particular type of forgery where a region of an image is copied and pasted onto the same image which is achieved to create duplication or to conceal some existing objects. To detect the copy-move forgery attack, Key-point based detection methods are used as it is said to be very effective in revealing copy-move evidences, due to their robustness against various attacks like large-scale geometric transformations. The results from the experiments reveal that the proposed technique precisely determines the copy-move compression and is able to effectively detect multiple copy-move forgeries. Two authentication bits are used i.e. block authentication and self-recovery bits are used to survive from the vector quantization attack. The insertion of self-recovery bits is done with Arnold transformation, which recovers the original image even after a high tampering rate. The proposed scheme is tested with different types of attacks such as text removal attack, text insertion attack and copy and paste attack. Hence the proffered technique provides a computationally efficient and dependable way of copy-move forgery detection which helps in increasing the credibility of images conspicuous centered applications.

KEYWORDS: Key-point based detection methods; vector quantization attack and Arnold transformation.

I. INTRODUCTION

The widespread emergence of computer networks and the popularity of electronic managing of medical records have made it possible for digital medical images to be shared across the world for services such as telemedicine, teleradiology, telediagnosis, and teleconsultation. Instant diagnosis and understanding of a particular disease also as lowering the amount of misdiagnosis has had extensive social and economic impact, clearly showing the necessity for efficient patient information sharing between specialists of various hospitals. In the handling of medical images, the main priority is to secure protection for the patient's documents against any act of tampering by unauthorized persons. Thus, the most concern of the prevailing electronic medical system is to develop some standard solution to preserve the authenticity and integrity of the content of medical images. Invisible watermarking methods can be divided into four groups: fragile, semi-fragile, robust, and hybrid methods. The fragile method allows the watermark to easily be destroyed by the smallest of modifications. Applications for this kind of watermarking are limited to authentication and integrity verification. The semi-fragile method protects the hidden data against intentional attacks, but is fragile against malicious attacks. The robust watermarking method, which is usually used for copyright protection purpose, should be resistant against multiple different attacks. The robustness of these methods can be measured by applying different attacks on the watermarked images and comparing the embedded and extracted watermark by different benchmarks. The lists of various attacks and benchmarks are introduced in the following sections. Finally, the hybrid watermarking is a mixture of robust and fragile techniques to provide authentication, integrity verification, and copyright protection simultaneously. In addition to above groupings, reversibility (also known as lossless or invertible watermarking) is another important aspect in watermarking. Compared to the normal watermarking schemes, reversible data hiding retrieves the watermark and also the primary multimedia perfectly, which can be a used as a critical requirement for medical and military applications. The main characteristic of reversible methods is that the ability to recover the first image with none distortion after extracting the watermark bits, besides providing tamper proofing and authentication. By employing a reversible data hiding algorithm to embed patient information and diagnostics data into the medical image, medical officers can recover perfectly both the hidden information also as the image itself.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

II. RELATED WORK

Basic Concepts in Watermarking Scheme

A. *Overview of a Data Security System*

The watermarking concept is closely related to two other fields: cryptography and steganography. These areas fall under the domain called data security system. Cryptography is a method for sending a message in a secure format that only the authorized person can decode and read. This is known as a "secret writing." Accordingly, one solution for tackling the above issue is the use of digital watermarking. In other words, watermarking can enhance the security of medical images by inserting special information, called a watermark or hidden data, in a non-conspicuous way. Watermark information is typically inserted during a binary format to the pixel value of the host image. This information can later be retrieved and checked whether the medical image is distributed with the actual source (authenticity) or belongs to the correct patient (integrity). Watermarking methods can be classified based on different views. In the following, different categories of watermarking methods are explained. Based on the embedding information concept, watermarking algorithms can be classified as either spatial or transform domain. In the spatial domain, the watermark information is directly embedded in the pixel value of the host or cover image. These methods are fast and simple and also provide high capacity for embedding watermarks. Spatial domain methods may have some advantages and may overcome cropping attacks, but their main drawback is their weaknesses against noise or lossy compression attacks. In addition, upon discovering the method, embedded watermarks can easily be modified by a third party. In the transform domain, the watermarked image is obtained by embedding the watermark onto the transformed version of the original image. Some of these transforms and a discussion on their benefits and weaknesses are provided in the following sections. According to human perception, the watermarking methods can be grouped into visible and invisible watermarks. A popular illustration of visible methods is logos, which are put at the corners of images or videos for content or copyright protection. Invisible watermarks are useful for application such as authentication, integrity verification, and copyright protection. Sometimes, visible and invisible watermarking can be used simultaneously. In this case, the invisible watermark can be considered as a backup for the visible one. This is called the dual watermarking technique. Even though the encrypted message can be protected during the transmission, once the message is decrypted, it is not protected anymore, and this is the main shortcoming of cryptography techniques when compared with watermarking. Furthermore, most of the cryptographic methods are complex and provide weak copyright protection property. Steganography is derived from the Greek word "steganos" and "graphei" which mean "covered" and "writing," respectively. In spite of some similarities between steganography and watermarking, there are some differences between them as explained below: The objective of steganography is to embed an unrelated secret message into a cover work, while in watermarking, the embedded information and cover work are related to each other. In steganography, the message should be invisible, but in watermarking, the embedded information can be either visible or invisible. The main goal of steganography is to hide the message into the cover data in a way so that an invader cannot detect it, while the main purpose of watermarking is to embed the data into the cover data in a way that it cannot be removed or replaced by an intruder. Based on these pros and cons, it can be concluded that watermarking is the best choice for preserving the security of a digital image. In addition, the data can be encrypted before embedding the watermark, as a second layer of protection.

B. *Different Parts of a Typical Watermarking System*

Digital watermarking is the procedure of embedding information (i.e., a watermark) into the host object in such a way that the watermark image/data can be detected by authorized individuals, for assertion of authenticity purposes. The host signal can be a video, audio, image, 3D mesh, etc., while the watermark can be a logo, image, serial number, owner's ID, name, or any other information which shows ownership of the host signal. These signatures are normally converted into a binary sequence before being embedding into the host signal. The following steps are the standard practice for the watermarking procedure.

- *Embedding:*
  In this part, the original image and the watermark enter to the system, and according to the embedding algorithm, the watermarked image will be produced.
- *Distribution:*
  The ability of others to access the water marked image. For instance, it can be sold to the customers or it can be published through the internet.
- *Attacks:*
  The modification of the watermarked image intentionally or unintentionally, by a third party. This concept will be explained in the next section.
- *Extraction:*
  The process of separating the hidden information from the water marked image. Extracting algorithms can be divided into three parts: non-blind, semi-blind, and blind. In non-blind or private watermarking, the original

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

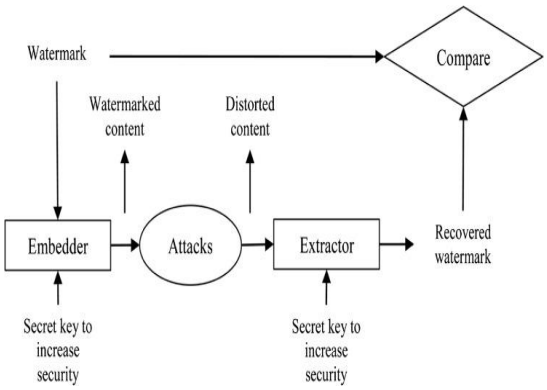
|| Volume 8, Issue 5, May 2020 ||

image is required during the extraction process. The original watermark or other side information is necessary to perform the extraction in semi-blind methods. In blind or public watermarking, the extraction process is done without any side information, original image, or original watermark.

- *Detection:*
  In this part, the quality of watermarked images and accuracy of extracted watermarks will be evaluated by measuring the similarity between the extracted and the original one.

C. *Distortion and Attacks on Watermarking System*

In image watermarking techniques, the main consideration is the evaluation of the robustness and effectiveness of the watermarking method through measurement of the impact of different attacks upon the watermarked image. Based on the watermarking method used, the image may be robust against a specific group of attacks. For instance, in order to increase robustness against geometrical attacks, Fourier-based methods may be a good solution. This section gives an overall vision on different groups of attack that may be used by invaders to remove the watermark from the watermarked image. These attacks, either intentional or unintentional, can be classified into two main classes: signal processing attacks and geometric distortion attacks.



D. *Digital Watermarking System Applications*

Watermarking algorithms are application dependent. Different algorithms have different restrictions and conditions. Some of the watermarking applications are given as follows:

- *Copyright Protection:*
  In this application, the owner's copyright information is invisibly inserted into the digital image, and ownership can be proven in the case of dispute, by extracting this information. For this, the watermark should be robust against legitimate and illegitimate attacks. This kind of watermark is not appropriate for preventing the user from making a copy of the digital image.
- *Fingerprinting:*
  In this application, the owner must embed different watermarks according to each customer identity. It means that the data, which are used as a watermark, will be chosen according to the customer's information. This method enables the owner to find the source of illegal copies and easily find the customer who breaks any license agreement. This watermark should be also robust and invisible.
- *Authentication and Integrity Verification*:
  The purpose of this application is to find out whether any modification has been done upon the digital image or not, and then localize the place of tampering. In this application, fragile or semi-fragile watermarking algorithms should be applied, which are not robust against content modification. Broadcast monitoring, content description, and covert communication are other applications of digital image watermarking.

E. *Digital Image Watermarking System Requirements*

In this part, the basic requirements for designing a general watermarking system are explained. For specific usage, such as in medical applications, some other features such as imperceptibility and reversibility must be added as explained fully in the medical part.

- *Fidelity:*
  This factor is used to determine the similarity between the watermarked and un-watermarked image. In other words, fidelity is the amount of imperceptibility of the watermark in the watermarked image.
- *Robustness:*
  In contrast to fragile watermarking, robustness implies resistance against a variety of innocent and malicious

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

attacks. Cropping, resizing, and compression are examples of unintentional attacks, which may commonly happen when processing a digital image. Noise addition and geometrical distortion are two instances of malicious attacks, which may be used by attackers to disable the watermark.

- *Data Payload (Capacity):*
  This factor shows the maximum amount of data, which can be embedded into an image without noticeably reducing image quality. The influence of capacity on the robustness and perceptibility of watermarked image is not negligible; for instance, by increasing the data payload, the robustness will decrease and the perceptibility will increase. The dimensions of the host image should also be considered, since the greater the image resolution, the greater is the amount of watermark is applicable in terms of bits.
- *Security:*
  This factor is regarding the application of the different kinds of keys, such as public or private, so that unauthorized persons cannot remove the watermark.
- *Computational Complexity (Speed):*
  This factor is regarding the computation time for embedding and extracting the watermark, which directly determines the computational complexity. For example, real-time application requires fast algorithms. However, for high-security applications, the embedding and extracting methods are usually more time consuming.
- *Perceptibility:*
  This factor is about the amount of distortion that appears on a watermarked image after inserting a watermark. For invisible watermarks, this factor should be as low as possible.

III. PROPOSED ALGORITHM

The proposed scheme locates image tampering also as recovers the first image. A host image is broken into 4×4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block wise SVD into the smallest amount significant bit (LSB) of the image pixels to work out the transformation within the original image. Two authentication bits namely block authentication and self-recovery bits are wont to survive the vector quantization attack. The insertion of self-recovery bits is decided with Arnold transformation, which recovers the first image even after a high tampering rate. SVD-based watermarking information improves the image authentication and helps to detect different attacked area of the watermarked image. In algebra, a QR decomposition (also called a QR factorization) of a matrix may be a decomposition of a matrix A into a product A = QR of an orthogonal matrix Q and an upper triangular matrix R. QR decomposition is usually wont to solve the linear method of least squares problem and is that the basis for a specific eigenvalue algorithm, the QR algorithm. Square matrix Any real square matrix A may be decomposed as

$$A=QR,$$

where Q is the orthogonal matrix (its columns are orthogonal unit vectors meaning Q QT = QT Q = 1) and R is the upper triangular matrix (also called right triangular matrix).

If A is invertible, then the factorization is unique if we require the diagonal elements of R to be positive. If instead A is a complex square matrix, then there is a decomposition

$$A = QR,$$

where Q is a unitary matrix (so Q Q* = Q* Q = 1)). If A has n linearly independent columns, then the primary n columns of Q form an orthonormal basis for the column space of A. More generally, the first k columns of Q form an orthonormal basis for the span of the first k columns of A for any $1 \le k \le n$. The fact that any column k of A only depends on the primary k columns of Q is liable for the triangular sort of R.

A. *Rectangular matrix:*

More generally, we can factor a complex $m \times n$ matrix A, with $m \ge n$, as the product of an $m \times m$ unitary matrix Q and an $m \times n$ upper triangular matrix R. As the bottom $(m-n)$ rows of an $m \times n$ upper triangular matrix consists entirely of zeroes, it is often useful to partition R, or both R and Q:

$$A = QR = Q = = Q_1R_1$$

where R_1 is an $n \times n$ upper triangular matrix, 0 is an $(m-n) \times n$ zero matrix, Q_1 is $m \times n$, Q_2 is $m \times (m-n)$, and Q_1 and Q_2 both have orthogonalcolumns.

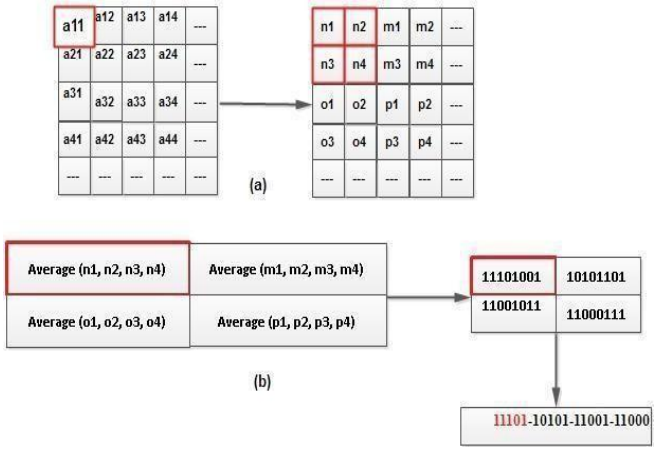
Golub & Van Loan (1996) call Q_1R_1 the *thin QR factorization* of A; Trefethen and Bau call this the *reduced QR factorization*.[1] If A is of full rank n and we require that the diagonal elements ofR_1 are positive then R_1 and Q_1 are unique, but in general Q_2 is not. R_1 is then equal to the upper triangular factor of the Cholesky decomposition of $A^* A$ ($= A^T A$ if A is real).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

IV. EXISTING SYSTEM

Abdulaziz Shehab proposed a new fragile watermarking-based scheme for image authentication and self-recovery for medical applications. This scheme locates image tampering as well as recovers the original image. A host image is broken into 4×4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block-wise SVD into the smallest amount significant bit (LSB) of the image pixels to work out the transformation within the original image. Two authentication bits namely block authentication and self-recovery bits are wont to survive the vector quantization attack. The insertion of self-recovery bits is decided with Arnold transformation, which recovers the first image even after a high tampering rate. SVD-based watermarking information improves image authentication and also provides a way to detect the different attacked areas of the watermarked areas. This scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared to the state-of-the art methods, this scheme greatly improves both tamper localization accuracy and the Peak signal to noise ratio (PSNR) of self-recovered image.



The host image is divided into small blocks of size 4×4 and the LSB of all these blocks are set as zero. This division guides us to calculate the tamper localization information for each block separately by the help of SVD operation on each 4×4 blocks. After SVD is computed for each block, the corresponding traces are also calculated. These calculated traces work because the Block Authentication Number (BAN) and wont to authenticate each block. The traces are mapped to the range of [0, 4095] in order to restrict the number of bits as 12, used for the trace's representation of each block. Further, block wise Arnold scrambling is performed and 4×4 blocks are again decomposed into 2×2 blocks. so that neighborhood block is recovered. The self-recovery information is calculated with the help of the average value of these 2×2 blocks. The obtained BAN and average value of Arnold scrambled 4×4 blocks are combined with each other with the help of a secret key in order to generate the complete watermark information. This complete watermark is inserted into the host image by replacing the last two LSBs of each 4×4 block (32 bits) with the generated watermark information of each 4×4block. The extraction process is quite similar to that of embedding process. Here are the details of step involved: Firstly, the watermarked image is divided into small blocks of size 4×4. As the LSB contained the watermarked information so it's separated out from the watermarked image then LSB is about as zero so as to re-calculate the Block Authentication Bits (12 bits). Then, BAN is calculated in the same way as calculated in embedding process. After that block-based scrambling is performed on this watermarked image with the same key as used during embedding process. The average value and self-recovery information is calculated in the same way as it is done in embedding. The calculated BAN and LSB extracted BAN are compared with other for each block along with the average information too. The blocks having same authentication bits are marked as not-tampered and rest are marked as tampered. Then, the tampered blocks information is recovered with the help of extracted self-recovery information from the extracted LSB data from watermarked image and finally the neighborhood block-based recovery is performed so as to enhance the self-recovery even further. This helps us to realize the improved self-recovery due to the very fact that neighborhood blocks of any image's pixels contain almost similar information.

A. *Arnold Transform Based Digital Image Sampling:*

The digital image can be considered as a two-dimensional matrix. When the size of the image is N, then I have $N \times N$ elements, the subscript x, y stands for the position of pixel, x, $y \in \{0, 1, 2..., N\text{-}1\}$. Let x, y corresponds to the x, y of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

Arnold scrambling, for each pair x, y, after all do Arnold Sampling, become x' and y', which equivalent to the original image of the point from (x, y) move to the = (x', y'), so realized the movement of pixels in the image, the image with Arnold Sampling traverse all the points to complete a picture of Arnold scrambling. The cycle of Arnold Sampling is relating to the size of the image, but not directly proportional. If size is 128 × 128-pixel image of Arnold scrambling cycle is 96, size 240 × 240-pixel image of Arnold scrambling for 60 cycles.

B. *Sampling Recovery in Arnold Sampling Algorithm:*

Arnold Sampling recovery has two ways: one is the application of its periodicity, and the other is the pursuit of its inverse matrix to the inverse transformation. It is very natural to leverage the periodicity of Arnold scrambling method. By research of it before, we can come to this conclusion: For the digital image of $N \times N$ pixels, as long as meet non-1 positive integer N, The Arnold Sampling has periodicity. Extend to an arbitrary Scrambling time of n, you need to proceed (mN-n mod mN) times Arnold Sampling transformation. However, the times of scrambling are related to the order of N, in general, if N is the number of higher-order cases, the cycle is relatively long.

C. *Singular Vector Decomposition:*

Today, singular value decomposition has spread through many branches of science, in particular psychology and sociology, climate and atmospheric science, and astronomy. It is also extremely useful in machine learning and in both descriptive and predictive statistics. Singular value decomposition is a method of decomposing a matrix into three other matrices:

$$A = USV^T \quad (1)$$

Where: A is an $m \times n$ matrix,

U is an $m \times n$ *orthogonal* matrix ,

S is an $n \times n$ *diagonal matrix*,

V is an $n \times n$ orthogonal matrix.

The reason why the last matrix is transposed will become clear later on in the exposition. Also, the term, "orthogonal," will be defined (in case your algebra has become a little rusty) and the reason why the two outside matrices have this property made clear. For the moment, we will assume that m ≥ n. What happens when this isn't true is quite interesting and is one of the keys, in my opinion, to understanding singular value decomposition. This is already becoming quite complicated so I will rewrite Equation (1) using summation notation. In this case, while it doesn't make anything simpler, it does make everything absolutely explicit:

$$a_{ij} = {}^{*} u_{ik} s_k v_{jk} .$$

Here, we've collapsed the diagonal matrix, S, into a vector, thus simplifying the expression into a single summation. The variables, $\{s_i\}$, are called singular values and are normally arranged from largest to smallest:

$$S_{i+1} \leq S_i .$$

The columns of U are defined as *left singular vectors*, while those of V are defined as *right singular vectors*. We know that U and V are orthogonal, that is:

$$U^T U = VV^T = I ,$$

where I is the *identity matrix*.

Identity matrix have the diagonal values as 1, with all other values being 0. Since U is not square, we cannot say that U Transpose$(U)=I$, so U is only orthogonal in one direction. Using the orthogonality property, we can rearrange (1) into the following pair of eigenvalue equations:

$$AA^T U = US^2 \quad (2) ,$$

$$A^T AV = VS^2 \quad (3)$$

D. *Numerical procedure:*

Since Transpose(A)A is the same size or smaller than A Transpose(A), a typical procedure is to plug Equation (3) into an eigenvalue calculator to find V and $S^2$and then find U by projecting A onto$V$:

$$A^T AV = VS^2 \quad (4).$$

Note that the method is completely symmetric; U and V change places when $A$is transposed:

$$A^T = V SU^T .$$

Thus, if $m < n$, we can transpose A, perform the decomposition, then swap the roles of U and V. In this scenario, U will be an $m \times m$ square matrix since there can be at most m non-zero singular values, while V will be an $n \times m$ matrix**.**

E. *LSB replacement:*

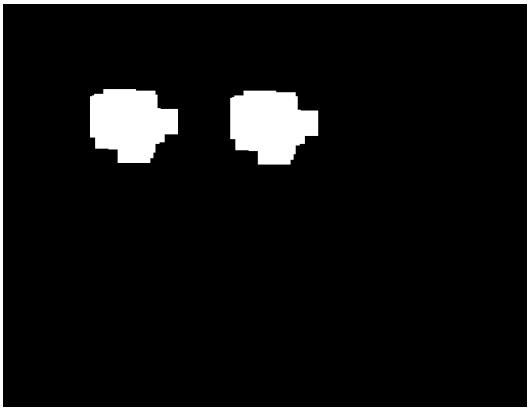
The cover image used is a color image. Before embedding the data, we use 8-bit secret key and XOR with all the bytes of the message to be embedded. Message is recovered by XOR operation by the same key. Every pixel value in the given image is analyzed and the following checking process proceeds. The Steps to be carried out for implementation of the technique is as follow. Let us consider the value of the pixel as gi, is in the range 240 <=gi<=255 then we embed 4 bits of secret data into the 4 LSB's of the pixel. This can be done by observing the first 4 Most

Significant Bits (MSB's). If they are all 1's then the remaining 4 LSB 's can be used for embedding data. If the value of gi (First 3 MSB 's are all 1's), is in the range 224 <=gi<=239 then we embed 3 bits of secret data into the 3 LSB's of the pixel. If the value of gi (First 2 MSB 's are all 1's), is in the range 192 <=gi<=223 then we embed 2 bits of secret data into the 2 LSB's of the pixel. And in all other cases for the values in the range 0 <=gi <=192 we embed 1 bit of secret data in to 1 LSB of the pixel. Similarly, we can retrieve the secret data from the values of an image by again checking the first four MSB 's of the pixel value and retrieve the embedded data. These steps have been carried out to get efficient results.

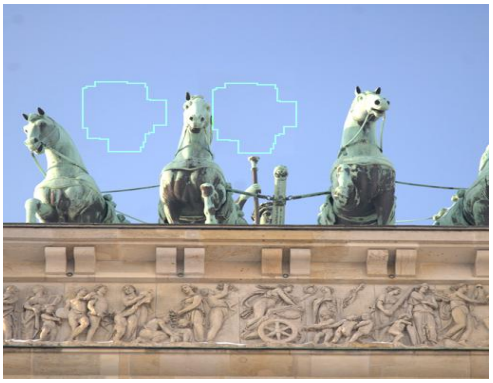
V. SIMULATION RESULTS

The Image Manipulation Dataset may be a ground truth database for benchmarking the detection of image tampering artifacts. It includes 48 base images, which consists of separate snippets from these images, and a software framework for creating ground truth data. The ultimate goal is to "replay" copy-move forgeries by copying, scaling and rotating semantically meaningful image regions. Additionally, Gaussian noise and JPEG compression artifacts are often added, both on the snippets and on the ultimate tampered images.

Fig(a) Processed data



Fig(b) Image tampering analysis



Fig(c) Forgery Comparison

VI. CONCLUSION AND FUTURE WORK

In this work, we have **p**roposed a fast and effective key point-based copy-move forgery detection and localization technique. This project presents a QR based fragile watermarking scheme using grouped block method to offer more security and provide a supplementary way to locate the attacked areas inside different medical images. Two authentication bits namely block authentication and self- recovery bits were used to survive the vector quantization attack. The usage of Arnold transform makes it possible to recover the tampered region from the neighboring blocks, which ultimately increases the NCC and PSNR of the recovered host.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 5, May 2020 ||

REFERENCES

1. Minerva M Yeung and Fred Mintzer. An invisible watermarking technique for image verification. In Image Processing, 1997. Proceedings, International Conference on, volume 2, pages 680– 683. IEEE,1997.
2. N Memon, S Shende and Ping Wah Wong. On the security of the yeung-mintzer authentication watermark. In IS and TS Pics Conference, pages 301–306. Society For Imaging Science & Technology,1999.
3. Matthew Holliman and Nasir Memon. Counterfeiting attacks on obliv- ious block-wise independent invisible watermarking schemes. Image Processing, IEEE Transactions on, 9(3):432–441, 2000.
4. Ping Wah Wong and Nasir Memon. Secret and public key image water- marking schemes for image authentication and ownership verification. Image Processing, IEEE Transactions on, 10(10):1593–1601,2001.
5. Chun-Shien Lu And H-YM Liao. Structural digital signature for image authentication: an incidental distortion resistant scheme. Multimedia, IEEE Transactions on, 5(2):161–173, 2003.
6. Shan Suthaharan. Fragile image watermarking using a gradient image for improved localization and security. Pattern Recognition Letters, 25(16):1893– 1903, 2004.
7. Toshihiko Matsuo and Kauro Kurosawa. On parallel hash functions based on block-ciphers. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 87(1):67–74,2004.
8. Ninghui Li, Wenliang Du and Dan Boneh. Oblivious signature- based envelope. Distributed Computing, 17(4):293–302, 2005
9. Shao-Hui Liu, Hong-Xun Yao, Wen Gao and Yong-Liang Liu. An image fragile watermark scheme based on chaotic image pattern and pixel- pairs. Applied Mathematics and Computation, 185(2):869–882, 2007.
10. Yu-Chen-Hu, Chun-Chi Lo, Chang-Ming Wu, Wu-Lin Chen and Chia-Hsien Wen. Probability-based tamper detection scheme for btc compressed images based on quantization levels modification. International Journal of Security and Its Applications, 7(3):11–32, 2013.
11. Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, Sung Wook Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, In Future Generation Computer Systems,
12. Jan, Z., Khan, A., Sajjad, M. et al. A review on automated diagnosis of malaria parasite in microscopic blood smears images, Multimedia Tools and Applications, 2017: 1–26. https://doi.org/10.1007/s11042-017-4495-2
13. R. Hamza, K. Muhammad, A. Nachiappan, and G. R. González, "Hash based Encryption for Keyframes of Diagnostic Hysteroscopy," IEEE Access, vol. PP1-1, 2017.
14. Hamza, R., Muhammad, K., Lv, Z., & Titouna, F. (2017). Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive and Mobile Computing.
15. Muhammad Sajjad, Khan Muhammad, Sung Wook Baik, Seungmin Rho, Zahoor Jan, Sang-Soo Yeo, Irfan Mehmood, Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource- constrained devices, Multimedia Tools and Applications, Volume 76, Issue 3, pp 3519–3536, 2017
16. Fita A* and Endebu B for Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection,2017.
17. Xinchun Cui, Yuying Niu, Xiangwei Zheng, Yingshuai Han for an optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image.

BIOGRAPHY

Ms.P.R.Hemalatha, working as Assistant Professor of CSE department in Velammal College of Engineering and Technology, Tamil Nadu, India. She received B.Tech degree in Information Technology from Raja College of Engineering and Technology, Madurai and M.Tech degree in Information Technology from K.L.N College of Information and Technology, Sivagangai. She has more than 8 years of experience. Her areas of interest include Ad-Hoc, Image Processing.

R.Kushmitha is a UG Scholar, Dept. of C.S.E, studying in Velammal College of Engineering and Technology, Madurai, India.

R.Sruthy is a UG Scholar, Dept. of C.S.E, studying in Velammal College of Engineering and Technology, Madurai, India

V.Vaishali is a UG Scholar, Dept. of C.S.E, studying in Velammal College of Engineering and Technology, Madurai, India.

V.Vaishnavi is a UG Scholar, Dept. of C.S.E, studying in Velammal College of Engineering and Technology, Madurai, India