INNOVATIVE LOW-COST PERIMETER SECURITY GADGET WITH IN-BUILT MECHANISM TO ENSURE CONFIDENTIALITY, AUTHENTICITY AND NON-REPUDIATION

Ritesh Mukherjee [1], Anirban Goswami[2], Soumit Chowdhury[3] and Nabin Ghoshal[4]

[1]Centre for Development of Advanced Computing, Kolkata, India
[2]Techno Main Salt Lake, Sec – V, Kolkata-700091, India
[3]Government College of Engineering & Ceramic Technology, Kolkata-700010, India
[4]Department of Engineering & Technological Studies, University of Kalyani, Kalyani-741235, West Bengal, India,

ABSTRACT

The concept is to capture and preserve the intruder's details in unattended mode. A camera is integrated with a processing unit and counter arrangement to ensure authenticity and non-repudiation of the captured images of the intruder before court of law. Ownership claim is justified concocting confidential data sharing of visual cryptography. Signal quality is retained and unauthorized tampering of secret data resisted. Entire procedure indulges: Message Digest M is generated using SHA-2 from the date and time stamp of the acquired image, two shares are generated from MAC address (K) of the network card and encryption is done using AES involving encoding using Hamming 1 – bit technique. The cover image is prepared in DCT domain to restrict JPEG compression. Sensitive data is embedded in restricted areas of DCT transformed image. Extraction of secret data verifies an intruder. The experimental results prove its efficacy over existing conventional system.

KEYWORDS

Visual cryptography, share generation, AES, key exchange, image compression.

1. INTRODUCTION

The term perimeter offers a defined boundary to act as the first line of defence against trespassers and Perimeter security has been an appropriate choice. But, the complexity of perimeter security depends on the valuation and surface area of a property. In modern times, electronic gadgets are widely used for perimeter security.

To be effective against well-heeled trespassers, active perimeter security and monitored CCTV are used to ensure both situation and customer requirements. Across the globe, property owners rely on surveillance systems in form of CCTV cameras to assist an individual in monitoring and protecting physical areas. But there is no specific template for a "perfect" perimeter detection system, due to the varying parameters like location, accessibility, points of entry, lighting and operational hours. So, recent technological advancement demands tailored surveillance system with maximum security and negligible human interference.

In the proposed algorithm, we have tried to amalgamate the hardware design of a self-developed security gadget with an inbuilt camera [1] having inbuilt processing unit to capture the facial image of a person with a timestamp.

The device has been framed with components having connectivity and functionalities defined as follows:

1. Portable Instrument cabinet: The main apparatus is an enclosure made of aluminium for necessary circuitry. This apparatus can be installed/commissioned in a hidden place. This box has got a built in mechanism for the following activities.

    - Capture continuous video.
    - Analyse frames to identify human faces.
    - Capture facial image and time information.
    - Transmit the captured facial image with a time stamp to the predefined offsite storage.

2. Gadget holding arrangement: This is a small sliding tray provided with the gadget to directly mount it.
3. Power supply module: The developed apparatus makes use of +5 volts regulated DC power supply up to a maximum 1000 mA current capacity. The Power supply module is a 5v micro USB power supply arrangement for the mentioned gadget.
4. Wi-fi dongle: Small USB wi-fi dongle which will be connected to the gadget and will help to transmit data from the portable gadget to the offsite storage in wireless mode.
5. Network cable [Optional]: A standard network cable with a RJ45 connecter will be used for the purpose of data transfer between a portable gadget and the offsite storage in wired mode. This will be useful as an alternate arrangement in absence of a reliable wireless arrangement.
6. Application Software: Above apparatus operates using application software. This application is responsible for headless start-up of the gadget, video capture, frame extraction, face detection, face image capture, time capture and transfer of facial images with a time stamp.

The gadget operates in following steps:

- Capture video of the rear view.
- Analysis of captured video in real-time.
- Detection of human faces from a captured frame.
- Crop face images.
- Capture time stamp (with index in case of presence of multiple faces on the same frame).
- Transfer facial images with a time stamp to offsite storage.

Basic requirements cum pre-requisites for the operation

- Power supply.
- Place for commissioning the gadget.
- Storage / Server with network connectivity (preferably wireless).

After capturing the facial image, we use the technique of visual cryptography and steganography for effective data hiding process.

2. LITERATURE REVIEW

To assure fidelity of a file [2. 3], data hiding techniques generally explain the fabrication of authentication signals in a digital file. Creators generally own the copyright to a digital image the

moment they create it like in physical mode. The owner is privileged with several exclusive legal rights over the use and distribution of it. The fabrication of the owner's key data as an invisible digital watermark [4, 5] in a digital file justifies the fact.

The concept of neural network-based visual cryptography helps to preserve the secrecy of data. To support visual cryptography, Shamir [6] proposed generation of public and private shares from secret information and subsequently shared the appropriate share. The secret data can only be revealed after bonding of appropriate shares. This justifies amalgamation of reversible data concealment [7] and encrypted information sharing to elucidate information security. In addition, Omnia Abdullah Alharbi et al. [8] supported conservative prevention of data through multilevel security pattern. In another algorithm, Sanjay Kumar et al. [9] mentioned recovery of cover media which justifies the authenticity of hiding.

Generally, data authentication protocols are implemented in the frequency domain and the DCT domain is most popular due to its efficient performance. Cox et al [10] proposed that DCT be used in the JPEG compression procedure. Moreover, resistance to JPEG compression was suggested by Koch et al [11] who used the middle band frequency coefficients of a DCT transformed block. The same concept was stated by Hsu et al. [12]. In another algorithm, Langelaar et al. [13] confirmed that the choice of middle-frequency bands for embedding restricts watermark information from getting scattered to low-frequency areas of the image. Lin et al. [14] explained resistance to JPEG compression by using a mid-frequency band of a DCT block for embedding.
The proposed approach has some exclusive features like:

1. A security gadget with an embedded camera is modelled to capture the facial image of an intruder and named with time a stamp.
2. The facial image is cropped from the captured frame, normalized in the desired format, and preserved with a date-time stamp.
3. Common terminologies about the security of the digital domain like Confidentiality, Integrity, and Availability in addition to Authenticity and Non- Repudiation to secure secret data with the combined effort of visual cryptography and steganography [15, 32].
4. The sensitive data is represented in a much more secure manner to ensure Confidentiality.
5. Use of middle-frequency band of a DCT transformed block for protecting the embedded secret data.
6. White noise is controlled by using a self-defined technique.
7. Both secrecy and security are ensured with negligible computational complexity in the case of share generation.
8. The 1-bit error detection and correction technique helps to retrieve the correct version.

The phase-wise elaboration of the protocol is done in the next section.

3. THE METHODOLOGY

3.1. Phase I

Every facial image collected through an inbuilt camera is cropped and normalized in the desired format and preserved with a date stamp. The date-time stamp is in the format of YYYY MM DDHHMISS [I] i.e. DT, where I is the index of the images.

3.2. Phase II

DT is digital data and using Sha-2[16] a 256-bit message digest is generated from DT i.e. DT#.

The gadget has a unique ID (say K) that is its 48-bit MAC address of either a wired or wireless card. It is represented as a string of bits say K_b which is of fixed length. With the help of a self-defined technique two shares KS1 and KS2 are pseudo-dynamically created from K_b. The bit ''1'' of K_b is represented as 0/1(KS1) & 1/0(KS2) and ''0'' as 0/1(KS1) & 0/1(KS2) respectively because K_b = KS1 XOR KS2. The bit sequence of KS1 and KS2 are generated pseudo-dynamically and so differs in content. KS2 cannot be generated from KS1 and even not vice versa. Even if a technically abled person with an ill intention tries to generate a duplicate version of KS1 and KS2, it cannot be done due to its pseudo-dynamic nature.

DT# is concatenated with KS2 to form DT#KS2.

Using K_b, DT#KS2 is encrypted by the technique of block cipher algorithm, i.e. AES (Advanced Encryption Standard) [16-18] with a key length of 256 bits to form $DT\#KS2_E$. Now $DT\#KS2_E$ and KS1 are encoded using Hamming 1-bit error detection and correction technique [19] to form $DT\#KS2_{EEC}$ and $KS1_{EC}$.

3.3. Phase III

In the proposed algorithm, we have tried to prevent data loss even after JPEG compression is affected. Firstly, the facial part of the image collected from the camera is partitioned as non-overlapping 8x8 blocks. The 8x8 blocks are levelled off and two-dimensional DCT is applied to them. Even after decompression, decent image quality is maintained at a quality level of 50 and is represented as a Q50 quantization matrix. Also, a technique of rounding off the fractional value further supports the prevention of data loss. The casting position in a middle-frequency band of every alternate block is always pseudorandom. So, the steps of Levelling, DCT, Quantize and round off help to avoid any data loss even after any JPEG compression attack on the modified image. These factors also prevent collusion attacks.

3.4. Phase IV

The embedding of $DT\#KS2_{EEC}$ and $KS1_{EC}$ is done in the mid-frequency range of the transformed block. $DT\#KS2_{EEC}$ is embedded in the diagonal part of the first and second 4x4 blocks and$KS1_{EC}$ is embedded in the diagonal part of the third and fourth 4x4 blocks of each 8x8 block.

3.5. Phase V

For authentication, the extraction algorithm executes on the facial image to be verified and performs the following steps to justify confidentiality:

1. $(DT\#KS2)`_{EEC}$ and $KS1`_{EC}$ are reframed internally in memory. Embedding technique as in phase III and subsequent extraction justifies confidentiality.
2. Now $(DT\#KS2)`_{EEC}$ is decoded to form $(DT\#KS2)`_E$ and $KS1`_{EC}$ is decoded to form KS1`using Hamming technique but within a private method.
3. Now $(DT\#KS2)`_E$ is decrypted using $K_b$ to form (DT#KS2)`. Further (DT#KS2)` is de-concatenated to form (DT#)` and (KS2)`.
4. Taking (KS2)` as input the algorithm will overlap with reframed KS1`and produce $K_{be,}$ which should match with K_b, to prove the authenticity of the image. Moreover, KS2 never leaves the gadget, the framed K_{be} matching with K_b ensures non-repudiation property.
5. This (DT#)`should match with the Sha-2 of the name of the file, i.e date and time stamp (YYYYMMDDHHMISS[I])of the image. To ensure, the integrity of the image is checked with the instant generated message digest from the date stamp of the facial image chosen.

The whole process is for the verification purpose of a captured facial image of an intruder with a date and time stamp.

4. DETAILED DISCUSSION OF THE OPERATIONAL STEPS

The description of the processes are:

4.1. Configuration of the device and its utility

The composition of the device is:

1) Process steps

- Capture video
- Extraction of frames
- Analysis of frame to detect face
- Crop face (if detected) and normalize
- Capture time information in 'ddmmyyyyhhmiss[I]' format
- Transfer cropped face image for offsite preservation.

The flow diagram of the steps is shown in figure 1.

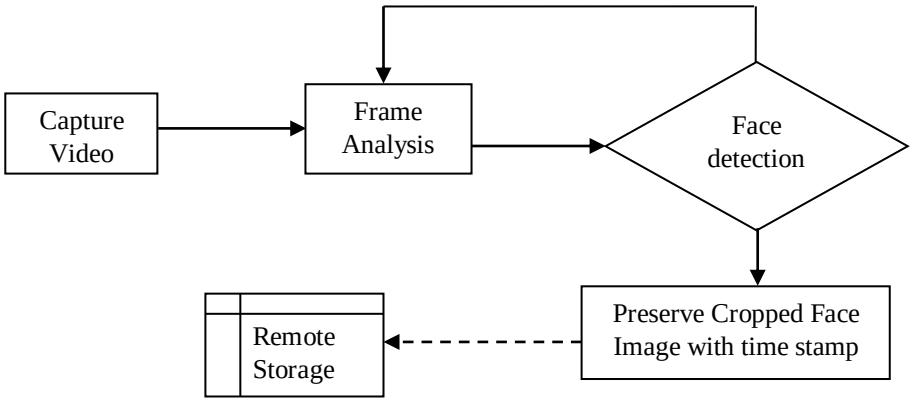

Figure 1. Brief flow diagram of the process

2) Product composition

- An aluminum cabinet.
- A digital video capturing and processing unit placed inside a metal housing
- A power supply module
- A holding means that includes a sliding tray arrangement for holding gadgets.
- Wi-fi dongle for transfer of cropped face image.
- Network cable for transfer of cropped face image (in absence of wireless connectivity)

3) All process parameters (for tested performance), more particularly those which are critical in the process

- Camera resolution: 320 X 240.
- Brightness: 60.
- Normalized face size: 80 X 80.
- Required storage: [1.84 -- 3.38] KB per image.

Figure 2 explains one possible implementation scenario where the gadget is installed in a residence to capture intruders' facial images and preserve them in dedicated storage for future reference. This type of installation is perfectly comparable with a low-cost domestic alternative of CCTV kind of arrangement.

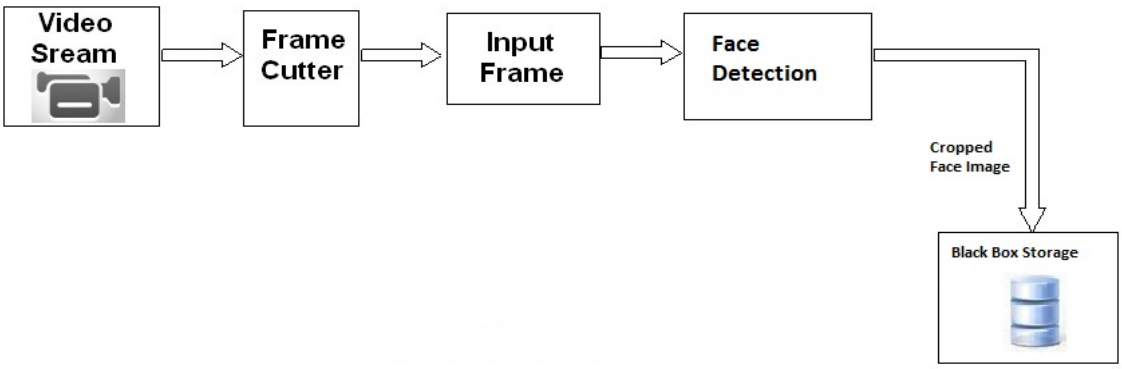

Figure 2. Implementation plan for surveillance of Individual's Residence

Figure 3 explains a scenario that may cover the deployment of the proposed gadget commercially where more than one gadget is installed at different strategic locations to capture the facial images of the trespassers and preserved in central storage, which may be in a compartmentalized manner for future reference. This type of implementation is suitable for the implementation of perimeter security in residential complexes and hotels etc.

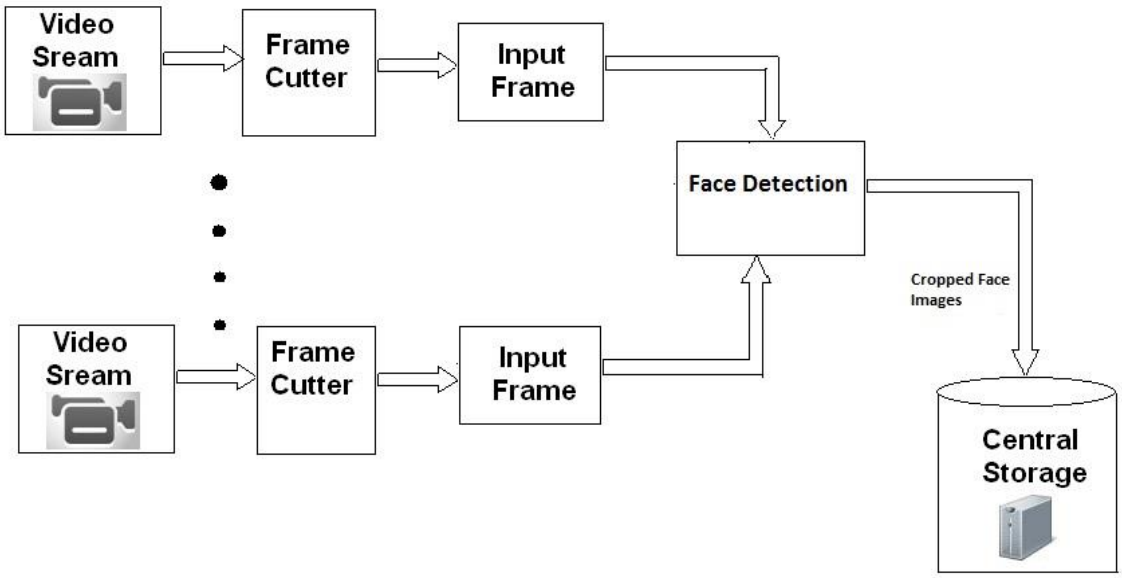

Figure 3. Implementation strategy for surveillance of Residential complex or Hotels

4.2. Cropping and Normalization of the captured Image

The facial image of a person is captured through the in-built camera and cropped to get a distinct facial image only.

Then, the image is normalized by changing the pixel intensity range. The motivation for the same is to achieve consistency and avoid mental distraction for the dynamic range of a given set of data (signals or images). The formula for normalizing a grayscale digital image is:

$$I_N = (I_O - I_{OMI}) * [(I_{NMA} – I_{NMI}) / (I_{OMA} - I_{OMI})] + I_{NMI} \quad (1)$$

Where

I_N = Normalized Image.
I_O = Original Image
I_{OMI} = Minimum pixel value of the original image.
I_{NMA} = Maximum pixel value of the new image.
I_{NMI} = Minimum pixel value of the new image.
I_{OMA} = Maximum pixel value of the original image.
I_{OMI} = Minimum pixel value of the original image.
I_{NMI} = Minimum pixel value of the new image.

In the proposed method, the values of I_{NMA} and I_{NMI} are taken as 255 and 0 respectively.

I_N is stored in the system with the date-time stamp in the format YYYYMMDDHHMISS[I]. It is in digital form and a 256-bit message digest (SHA-2) is generated from it.

4.3. Generation of Shares

The 48-bit MAC address of a wired or wireless card is represented as a bit sequence and considered for the generation of shares.

The format of two shares (KS1 and KS2) depends on the intensity value defined by PI(x, y). To generate the shares “0” is represented as “0” and “1” is represented as “255”. The conversion is due to the framing of black and white pixels which will help to reconstruct the MAC address even after some image processing operations are applied as proposed by Tai-Wen Yue et al. [15].

The shares are generated as: (PI(i,j)==0) ? KS1(i,2*j-1) = 255, KS1(i,2*j) = 0, KS2 (i, 2*j-1) = KS1 (i, 2*j), KS2(i, 2*j) = KS1(i, 2*j-1) : (mod (random ([m n]), 2) == 0) ? KS1(i, 2*j-1) = 255, KS1(i,2*j) = 0, KS2(i, 2*j-1) = KS1(i,2*j-1), KS2(i, 2*j) = KS1(i,2*j): KS1(i,2*j-1) = 0; KS1(i,2*j) = 255, KS2(i, 2*j-1) = KS1(i,2*j-1),S2(i,2*j)= KS1(i,2*j); (2)

Here, r and c represent the width and height of payload data, i varies from 1 to r and j varies from 1 to c. The values of m and n are taken arbitrarily depending on the corresponding pixel intensity. The procedure of share generation from 48 bits MAC address is shown in figure 4.

AA.F0.C1.E2.77.51	10101010.11110000.11000001.11100010.01110111.01010001	**Conversion of 0 to 0 and 1 to 255**	 Share 1  Share 2	**Sequence of 0 and 255**
48 bit MAC address	**Binary format of MAC address**	**Gray scale Image (Fabricated)**	**Generation of shares**	**Gray Scale Image (Detected)**

Figure 4. Share Generation

4.4. Formation of Message digest and it's encryption

Secured Hashing Algorithm (SHA) variant 2 is much more secure because it generates a unique value for every digest. A 256-bit hash value denoted as DT# is generated from DT. DT# is concatenated with KS2 to form DT#KS2.

Due to the involvement of a lesser number of bits in the encryption process as in DES technique, a more robust form of encryption is Advanced Encryption Standard (AES). This is a variant of the Rijndael block cipher which enhances the encryption technique to give the best protection for sensitive data from prying eyes.

In the proposed algorithm, we have taken consecutive blocks from DT# each of size 128 bits. i.e. AES technique which separates the data into a four-by-four column of sixteen bytes. This format explicitly considers the allowed values for the key length (Kl), block size (Bs) and the number of rounds (Rn) to be 8,4 and 14 respectively. Moreover, AES is a symmetric encryption algorithm and the same key K_b represented as 128 bits are used for the encryption and decryption process.DT#KS2 is encrypted to form $(DT\#KS2)_E$.

For execution, the AES-256 algorithm uses a round function and involve four different byte-oriented transformations:

1) Byte substitution using a substitution table (S-box).
2) Shifting rows of the State array by different offsets.
3) Mixing the data within each column of the State array.
4) Adding a Round Key to the State.

The intended receiver knows the symmetric key.

The motive behind the use of the AES mechanism is that: 1) The image encrypted can only be deciphered by the receiver as the key is only known to the sender and receiver.2) AES technique proves better because a block is processed as a whole to frame the ciphertext.3) The key expansion method makes it more robust.

This technique provides enhanced confidentiality and is quite strong concerning the conventional approaches.

4.5. Encoding using Hamming 1-bit error detection and correction technique

Hamming code uses the block code technique to encode a message. Some redundant bits are taken and inserted at specific locations in a message for error detection and correction. The receiver receives a message and checks the bit position for error.
The redundant bits are determined as: $2^r \geq m + r + 1$ where *m* is the number of data bits and *r* is the number of redundant bits. This is explained by Ramadhan J. Mstafa et al. [19].

For example, if the data to be encoded is 1011001, the redundant bits are R8, R4, R2, and R1 and will be combined with the data bits to form 101R8100R41R2R1.

In the algorithm, Hamming Code is used on a 3-bit code. We can assume a single bit as a set of 8 bits and pad an extra bit at the 9^{th} position to get a set of 9 bits. Now 3 consecutive bits are put to manipulation using Hamming Code and the procedure is followed for encoding at the sender's end and decoding at the receiver's end. As per the formula, if there are 3 data bits then including 3 redundant bits the total bit set will of 6 bits (3 + 3).

In our algorithm, we have considered a data set of three bits at a time. For example, if the data set is D2D1D0 and check bit set is C0C1C2, then the encoded word will beC0C1D2C2D1D0. The weightage of C0, C1, C2 are calculated as:

C0 = 0, D2D1 = 00 or 10,
= 1, D2D1 = 01 or 11.
C1 = 0, D2D0 = 00 or 10,
= 1, D2D0 = 01 or 11.
C2 = 0, D1D0 = 00 or 10,
= 1, D1D0 = 01 or 11. (3)

After all the bits of $(DT\#KS2)_E$ and KS1 are encoded we get $(DT\#KS2)_{EEC}$ and $KS1_{EC}$.

4.6. Generation of pseudorandom embedding point

A variable ipos is generated pseudo-randomly for the embedding of secret bits. A particular block (k) as determined by mod (k, 2) is chosen for embedding. The mathematical derivation for ipos is done as:

ipos = (I_n), n varies from 1 to 8.
$B_1 = I_0I_1I_2I_3$.
d1 = (I_0I_1) XOR $(I_2I_3) = d_{11}d_{12}$.
k = K_n, n varies from 1 to 8.
$B_2 = K_0K_1K_2K_3$.
d2 = (K_0K_1) XOR $(K_2K_3) = d_{21}d_{22}$.
d3 = d1 XOR d2 = $d_{31}d_{32}$.
ipos = Dec (d3) = any value from 0 to 3.
ipos= (ipos == 0 || ipos ==1) ? 1: (ipos == 2)? 2:3. (4)

Here B_1 and B_2 are the combination of 4 bits. d1, d2 and d3 are the intermediate values owing to bit operations.

4.7. Embedding Technique

Input: The facial part of the Image as cover and $(DT\#KS2)_{EEC}$ and $KS1_{EC}$ as the payload.

Output: An authenticated Image.

The facial image is considered as a set of non–overlapping 8 x 8-pixel blocks. Firstly the blocks are prepared to resist loss through JPEG compression and then they are used individually for the embedding of the full payload.

Step 1: The technique of DCT is effective within the pixel intensity range of -127 to 128 and so the pixel values are leveled off by subtracting 128 from them individually.

Step 2: The values [–127 128] of a block are converted to frequency components on the application of the forward DCT formula (Equation 5).

$$Bpq=\alpha_p\alpha_q\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}Amn\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}$$, where 0≤ p≤ M-1 and 0≤q≤N-1. (5)

The terms α_p and α_q are represented as,

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{2}/M, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{2}/N, & 1 \le q \le N-1 \end{cases}$$

Using the above formula, Bpq are obtained from Amn.

Step 3: The frequency coefficients are quantized by using a matrix Q50 and rounded off to the nearest integer. This is done to distribute the energy of an image in low, medium and high-frequency zone. Distortion in the low-frequency area produces visual alterations but the high-frequency zone is untouched by the JPEG quantizer. In the proposed algorithm, parametric modifications of the coefficients control share casting with an eye on resisting JPEG compression [31].

Step 4: Coefficients in the middle-frequency zone are chosen pseudo-randomly depending on:

(flag == true) ? (S1(w) == 0) && (ipos == i) ? CI(i, 7-i) < 0 ? diff = 0 - CI(i, 7-i), CI(i, 7-i) = CI(i, 7-i) + (diff + d) : (CI(i, 7-i) == 0) ? CI(i, 7-i) = CI(i, 7-i) + d : CI(i, 7-i) = CI(i, 7-i) : (S1(w) == 255) && (ipos == i) ? CI(i, 7-i) > 0 ? diff = CI(i, 7-i) – 0, CI(i, 7-i) = CI(i, 7-i) - (diff + d) : (CI(i, 7-i) == 0) ? CI(i, 7-i) = CI(i, 7-i) - d : CI(i, 7-i) = CI(i, 7-i) : Index values of CI are swapped for both black and white intensity values of S1(w). (6)

The assumptions are:

1. For similar value of ipos, the index values of CI are alternated by using a flag variable.
2. S1(w) denotes the payload vector at position w. Here the payload vector is $DT_{\#EE}$ and $KS1_E$.
3. The value of i is equivalent to ipos.
4. CI(i, 7-i) is the intensity value of the cover image pixel at location (i, 7-i).
5. The value of d helps to maintain an acceptable image distortion even after hiding i.e. imperceptible to HVS.

$DT_{\#EE}$ is embedded in the diagonal part of the first and second 4x4 blocks and $KS1_E$ is embedded in the diagonal part of the third and fourth 4x4 blocks of each 8x8 block.

Step 5: Restoration is done by the product of the current block and Q50.

Step 6: The generated values of a block are rounded off to the nearest integer after applying Inverse DCT (IDCT) (equation 7).

$$Amn=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}\alpha p\alpha q\, Bpq \cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}$$, where 0≤m≤M-1 and 0≤n≤N-1. (7)

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{2}/M, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{2}/N, & 1 \le q \le N-1 \end{cases}$$

Next, 128 is added to each value to complete the decompression procedure. The generated 8x8 block is returned to its original location. After all the blocks are properly rewritten, the image is reframed to form an authenticated image.

4.8. Payload Detection Process

Input: An authenticated image.
Output: An authentic Image.

The input image is considered as a set of non – overlapping 8 x 8 pixel blocks. The choice of blocks is similar to that done in the hiding process. The following steps are repeated for the total detection of the payload.

Step 1: To make DCT coefficients robust, 128 is subtracted from all the values of 8x8 blocks of the image.
Step 2: 2D DCT is applied to the levelled-off blocks.
Step 3: To resist JPEG compression, a standard matrix Q50 is used to quantize each matrix.
Step 4: Mid frequency region coefficients are pseudo-randomly chosen for extraction of the bits.
Step 5: The detection of the bits is accomplished as:

(flag == true) ? (ipos == i) ? (WI (i, 7-i) > 0)? S1E (w) = 0: S1E (w) = 255.
(flag == false) ? (ipos == i) ? (WI (7-i, i) > 0)? S1E (w) = 0: S1E (w) = 255. (8)

Here WI represents the pixel intensity and S1E represents the payload vector.

Step 6: The determination of bit (0/1) is done by flag variable. Subsequent 8 bits form a byte and the subsequent bytes are placed consecutively to check for their correctness.
In the proposed algorithm $(DT\#KS2)`_{EEC}$ and $KS1`_{EC}$ are reframed internally and through Hamming process $(DT\#KS2)`_{E}$ and KS1` are obtained and restored internally. $(DT\#KS2)`_{E}$ is decrypted to form (DT#KS2)`. After de-concatenation, we get (DT#)` and (KS2)`.
Step 7: (KS2)` is overlapped with KS1` to produce K_{be}. If K_{be} matches with K_b, the collected image proves the presence of the intruder. Moreover, as (KS2)` never leaves the gadget, the match also ensures the non-repudiation property of the gadget.
Step 8: To ensure the integrity of the image, the (DT#)` is matched with Sha-2 that is generated from date and time stamp of the facial image chosen.

The flow chart in figure 5 is the pictorial representation of sub-sections 4.2 to 4.7 respectively.

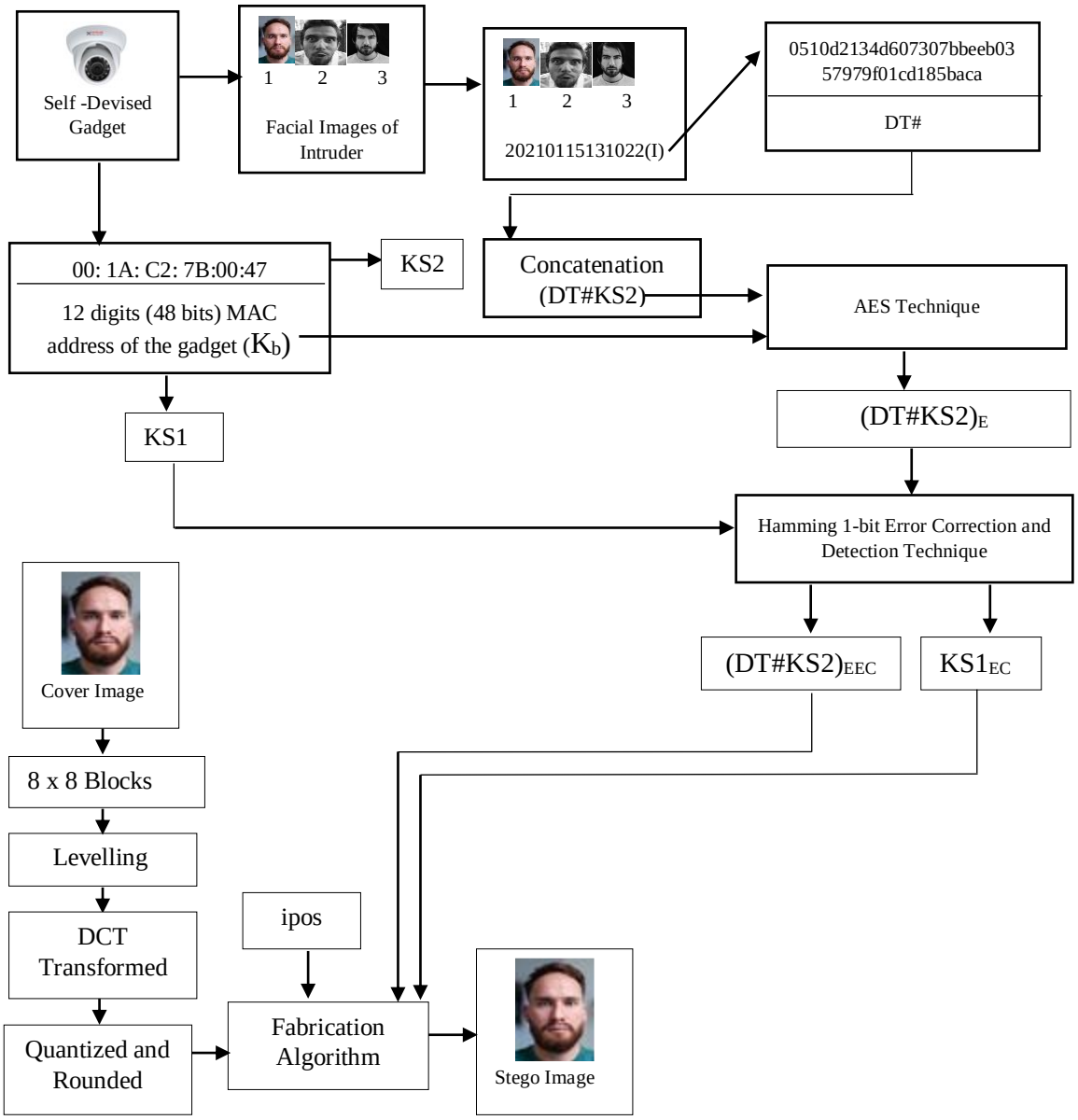

Figure 5. Procedure performed for Data Hiding

The flow chart in figure 6 is the pictorial representation of sub-section 4.8 respectively.

=

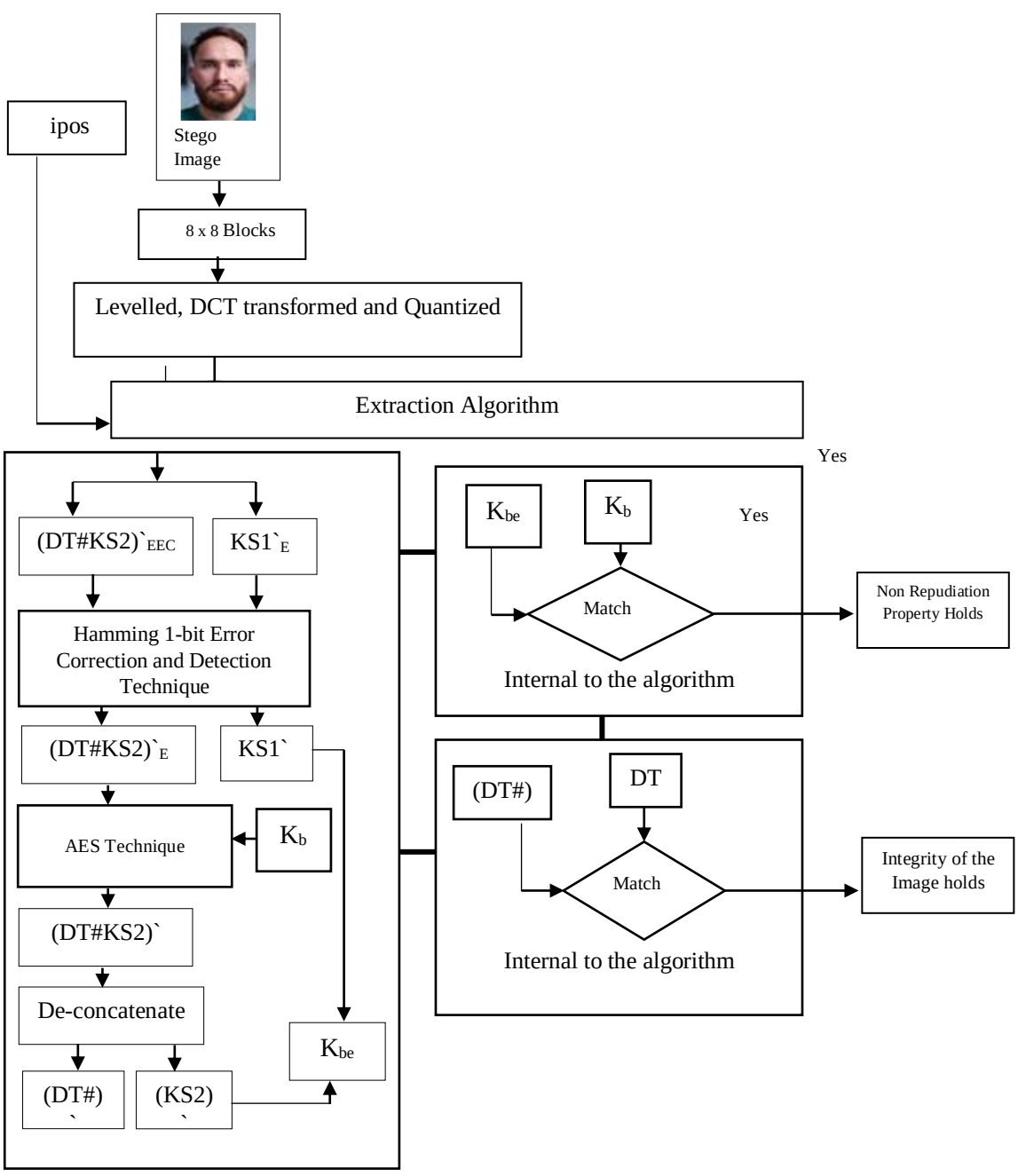

Figure 6. Procedure performed for Authentication

5. COMPLEXITY ANALYSIS

The proposed algorithm aims at developing a low-cost device to detect and justify the presence of an intruder. The justification of presence has been achieved through amalgamation of visual cryptography and steganography in digital medium and so the complexity factor may not be much of a concern. The self-defined procedures have less amount of mathematical and computational complexity as compared to conventional procedures.

To justify:

- DCT transform is used to convert spatial format to frequency format and hence the image information exists in a quantitative form beneficial for compression manipulation. This helps in Human Visual System.
- In the context of visual cryptography, a self-defined procedure is defined to create two shares. Instead of power and modulus, we chose an approach that is less complex and robust. As the time complexity to generate the shares is each O(n2I).
- The reason for using Hamming code is to establish copyright and sensitive data protection religiously.
- The features of data communication can be customized for commercial benefit.
- AES mechanism has been chosen for all its improved features, except the complexity factor.

6. PERFORMANCE ANALYSIS

6.1. Result Analysis using Image quality Metrics

Certain standard grayscale facial images are taken for verifying the effectiveness of data insertion and extraction methods. Matlab (version R2020a) is used for coding. The dimension of the source images is taken as 512 x 512. Some of the sources and corresponding authenticated versions are shown in figure 7.

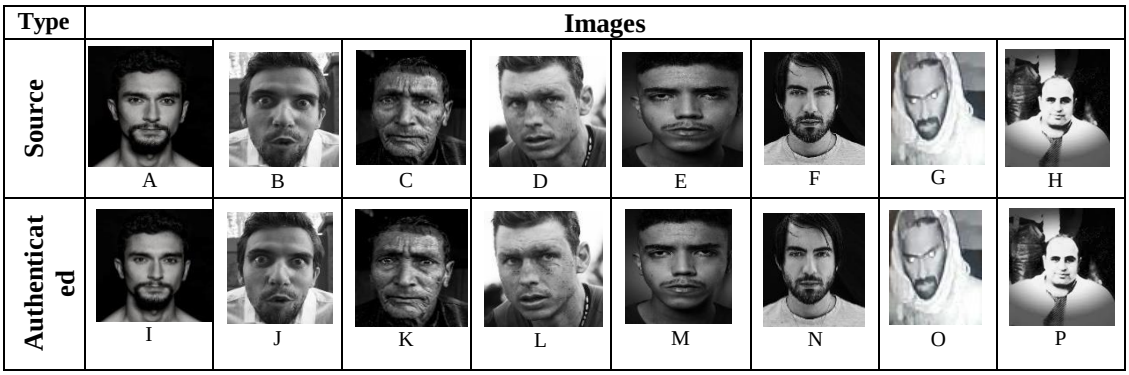

Figure 7. Visual Interpretation

The source and authenticated images are visually identical, despite using the mid-frequency band to hold secret data.

The algorithm has restricted Visual Attacks by manipulating white noise. Further, the efficiency of the algorithm is tested with the image quality metrics like, Mean Square Error (MSE) [20], Peak Signal to Noise Ratio (PSNR) [20], Image Fidelity (IF), Structural Similarity Index Metric (SSIM) [21], Bit Error Rate (BER) [22] and Normalized Correlation Coefficient (NCC) [21]. In table 1, the values are mentioned according to the metrics.

Table 1. Performance Analysis

Images	MSE	PSNR	IF	SSIM	NCC
A	8.2912	42.4101	0.9371	0.9914	0.9941
B	7.3109	43.9102	0.9313	0.991	0.9902
C	8.2912	42.4101	0.9371	0.9914	0.9941
D	7.3109	43.9102	0.9313	0.991	0.9902
E	8.2912	42.4101	0.9371	0.9914	0.9941
F	7.3109	43.9102	0.9313	0.991	0.9902
G	8.2912	42.4101	0.9371	0.9914	0.9941
H	7.3109	43.9102	0.9313	0.991	0.9902
Average	**7.80105**	**43.16015**	**0.9342**	**0.9912**	**0.99215**

The achieved average PSNR value is 43.16 dB is quite acceptable. The computed values of MSE, IF, SSIM, and CC i.e. 7.801, 0.934, 0.991, and 0.992 respectively justify closeness between the original and authenticated images w.r.t HVS. The values of table 1 also interpret the high possibility of sensitive data recovery during authentication.

6.2. Effectiveness against other techniques

The effectiveness of the algorithm has been based on modelling a low-cost device as the hardware component and establishing accurate proof of evidence of the presence of the intruder. The second part has been dealt with accurately based on secured generation of shares, encrypting the sensitive data in the best possible method, the accurate embedding of sensitive data and possible authentication as and when required.

In addition, the proposed algorithm is compared with similar existing techniques w.r.t PSNR as in table 2. The average PSNR value shows that the proposed technique is quite acceptable.

Table 2. PSNR comparison

Sl. No.	Algorithms	Resolution Level	PSNR (in dB)
1	[23]	1	29.01
2	[24]	2	34.82
3	[25]	2	31.10
4	[26]	2	24.51
5	[27]	1	35.41
6	[28]	2	22.78
7	[29]	2	36.16
8	[30]	1	37.61
9	**Proposed**	**2**	**43.16**

6.3. Resistance against Attacks

Statistical Attack: The fabrication intensity is properly verified to resist any significant distortions in the authenticating signals. Considering C_S, M_S, and t as a carrier signal, modified signal and intensity strength respectively the mathematical interpretation is $M_S = t \times C_S$. To sustain imperceptibility and robustness in fabrication, the intensity of t is attuned to control white noise. To justify, the density estimation is compared between the original and authenticated images as in figure 8.

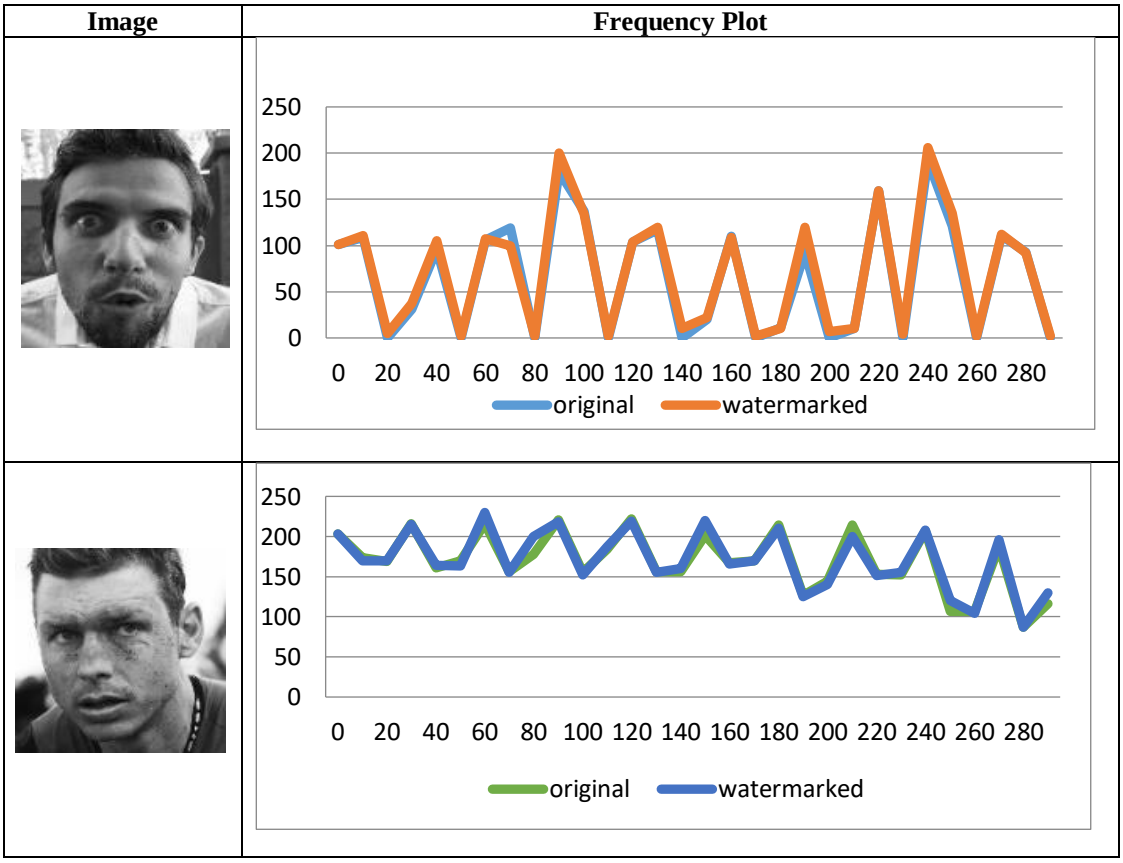

Figure 8. Analysis based on Frequency Distribution

Figure 8 shows a negligible difference between the original and the authenticated images.

Copy Attack: A copy of the authenticated image and the original image may be available to an intruder. If compared, the two files will be different. But as one of the shares is held by an intended receiver, it is never possible for an attacker to destroy the hidden information. The procedure during authentication is internal. Even if the authenticated images are hacked by an intruder bit error is incorporated, Hamming 1 – bit error detection and correction technique can easily rectify it. Also, a similar symmetric key cannot be generated by an intruder which helps to resist copy attack. In addition, the cover image also varies and hence restricts protocol attack.

Collusion Attack: The attacker may have an intention to destroy the content of a document by combining the copies of it. But in the proposed algorithm, the embedding position is pseudo-random in every context and so whatever may be the number of authenticated images, combining them all will not help to decipher the sensitive portion. The average technique implemented on the multiple copies of the same authenticated image is $g(x, y) = f(x, y) + n(x, y)$, where $f(x, y)$ is the original, $g(x, y)$ is the noisy image and $n(x, y)$ is the amount of noise added. In this algorithm $g(x, y)$ will never converge to $f(x, y)$ and $n(x, y)$ not having the value "0". The authenticated users are only privileged to authenticate the presence of an intruder.

Normalized-Cross correlation (NCC): The intensity variation is checked between the original and authenticated images. A value close to 1 justifies the closeness of extracted sensitive data to the actual signal. Table 3 shows the NCC value of the extracted sensitive data after certain attacks.

Table 3. NCC value comparison after attacks

Applied attacks names with their respective parameter values	NCC values of four recovered signatures copies were found from different regions of the cover image
Vertical Flip – 180^0 and then reverse	0.9994
Horizontal Flip – 180^0 and then reverse	0.9995
Blurring (Blur Radius – 5, Max Delta – 2)	0.9206
Gaussian Filter (Filter - 3*3 & Sigma – 0.9)	0.8069
Circular Average Attack (radius 0.5)	0.9115
Normalization	0.9645

7. CONCLUSION

The proposed method emphasizes introducing a low-cost device to capture and preserve the presence of an unwanted person in unattended mode and also to establish the presence of the intruder. The key factors are:

1. The embedding is done to prevent loss of data due to JPEG compression.
2. The embedding positions are pseudorandom in nature.
3. The encryption of message digest (SHA-2) by the AES mechanism before embedding helps to protect sensitive data from an intruder.
4. The content of the shares is different from each other and depends on their generation at different times.
5. If an error occurs in one bit, it can be easily rectified by Hamming code technique.
6. One of the shares is never public and difficult to obtain by an intruder.
7. The average PSNR value of 43.36 dB and NCC value of 0.93 clearly shows an advancement in frequency domain-based data security.

Hence, the efficacy lies in lost cost devices, improved robustness, secured hiding and low visual artifacts. But, this algorithm can be further extended to include the following:

- Use of multi-bit error correction technique with Cyclic Redundancy Check and Hamming Distance.
- Non-overlapping of multi-copy of secret data in different segments of the cover medium.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENTS

The author(s) expresses their deep sense of gratitude towards all the faculty and staff members of the Department of Engineering & Technological Studies, University of Kalyani, West Bengal, India, for their kind cooperation and support in connection with carrying out this research work.

REFERENCES

[1] Debasis Mazumdar & Ritesh Mukherjee (2020) “Apparatus for Automated Monitoring of Facial Images and a process therefor”, US Patent 10,592,727, filed April 21, 2015 and issued Mar 17, 2020.

[2] Lu C.S. & Liao H.Y.M. (2001) “Multipurpose watermarking for image authentication and protection”, IEEE Transactions on Image Processing, Vol. 10, No. 10, pp. 1579–1592.

[3] Yu G.J., Lu C.S. & Liao H.Y.M. (2001) "Mean quantization-based fragile watermarking for image authentication", Optical Engineering, Vol. 40, No. 7, pp. 1396–1408.
[4] Barni M., Bartolini F. & Furon T. (2003) "A general framework for robust watermarking security", Signal Processing, Vol. 83, No. 10, pp. 2069–2084.
[5] Lee I.S. & Tsai W.H. (2009) "A new approach to covert communication via PDF Files", Signal Processing, Vol. 90, No. 2, pp. 557–565.
[6] Shamir A (1979) "How to share a secret", Communication of the ACM, Vol.22, No.11, pp. 612–613.
[7] Brabin, D. R. D., Perinbam, J. R. P. & Meganathan, D. (2016) "A block-based reversible data hiding scheme for digital images using optimal value computation", Wireless Personal Communications. DOI: 10.1007/s11277-016-3817-4.
[8] Omnia Abdullah Alharbi, Asia Othman Aljhadli & Azizah Abdul Manaf (2020)"A Robust Double Layer Steganography Technique Based on DNA Sequences", The 4th International Conference on Future Networks and Distributed Systems (ICFNDS), article No.:38, pp.1–5, https:// doi.org / 10.1145 / 3440749. 3442644.
[9] Sanjay Kumar, Anjana Gupta & Gurjit Singh Walia (2021) "Reversible data hiding: A contemporary survey of state-of-the-art, opportunities, and challenges", Applied Intelligence, Vol.52, issue 7, pp 7373–7406, https://doi.org/10.1007/s10489-021-02789-2.
[10] Cox I J, Kilian J, Leighton T & Shamoon T (1997) "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transaction on Image Processing, Vol. 6, No. 12, pp. 1673–1687.
[11] Koch E & Zhao J (1995) "Towards robust and hidden image copyright labeling", Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, pp. 452–455.
[12] Hsu C. T. & Wu J. L. (1999) "Hidden Digital Watermarks in Images", IEEE Trans. On Image Processing, Vol. 8, No. 1, pp. 58-68.
[13] Langelaar G., Setyawan I. & Lagendijk R.L. (2000) "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Vol. 17, pp. 20-43.
[14] Lin S. D., Shie S. C. & Guo J. Y. (2010) "Improving the robustness of DCT based image watermarking against JPEG compression", Computer Standards & Interfaces, Vol. 32, pp. 54–60.
[15] Yue T. W. & Chiag S. (2000) "A Neural Network Approach for Visual Cryptography", IEEE-INNS-ENNS International Joint Conference on Neural Networks, Vol.5, pp. 494-499.
[16] Jayeeta Majumder & Chittaranjan Pradhan (2020) "Pixel Value Differencing Based Image Steganography using AES and SHA-2 Cryptography Method", International Journal of Recent Technology and Engineering (IJRTE), Vol. 8, No. 5, pp. 5325-5329.
[17] Roshni Padate & Aamna Patel (2014) "Encryption and Decryption of Text using AES Algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, No. 5, pp. 883-886.
[18] M.Pitchaiah, Philemon Daniel & Praveen (2012) "Implementation of Advanced Encryption StandardAlgorithm", International Journal of Scientific & Engineering Research, Vol. 3, No. 3, pp. 1-6.
[19] Mstafa R J & Elleithy K M (2014) "A Highly Secure Video Steganography using Hamming Code (7, 4). Systems", Applications and Technology Conference (LISAT), IEEE.
[20] Varnan C S, Jagan A, Kaur J, Jyoti D & Dr. Rao D S (2011) "Image Quality Assessment Techniques on Spatial Domain", International Journal of Computer Science and Technology (IJCST), Vol. 2, No.3, ISSN: 2229-4333(Print), ISSN: 0976-8491(Online).
[21] Wang Z, Bovik A C, Sheikh H R & Simoncelli E P (2004) "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transactions on Image Processing, Vol.13, No.4.
[22] Kaur G & Kochhar A (2011) "A Steganography Implementation based on LSB and DCT", International Journal for Science and Emerging Technologies with Latest Trends, Vol.4, No.1, pp. 35–41. ISSN No: Online 2250-3641.
[23] S. D. Lin, S. C. Shie & J. Y. Guo (2010) "Improving the robustness of DCT based image watermarking against JPEG compression", Computer Standards &Interfaces, Vol. 32, pp. 54–60.
[24] S. D. Lin & C. F. Chen (2000) "A robust DCT based watermarking for copyright protection", IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp. 415–421.
[25] S. D. Lin, S. C. Shie & C. F. Chen (2003) "A DCT based image watermarking with threshold embedding", International Journal of Computers and Applications, Vol. 25, No. 2, pp. 130–135, 2003.
[26] Vikash Saxena & J. P. Gupta (2009) "A novel watermarking scheme for JPEG images", WSEAS Transactions on Signal Processing, 2009, Vol. 5, No. 2, pp. 74–84, 2009.

[27] Rekha Chaturvedi, Abhay Sharma, N. Hemrajani & D. Goyal (2012) "Analysis of robust watermarking technique using mid-band dct domain for different image formats", International Journal of Scientific and Research Publications, Vol. 2, No. 3, pp. 1–4.
[28] Q. Kang, K. Li, & J. Yang (2014) "A digital watermarking approach based on DCT domain combining QR code and chaotic theory", in Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1–7.
[29] Jobin Abraham & Varghese Paul (2016) "A DCT based imperceptible color image watermarking scheme", International Journal of Signal Processing, Image Processing, and Pattern Recognition, Vol. 9, No. 7, pp. 137–146.
[30] Anirban Goswami, Ritesh Mukherjee & Nabin Ghoshal (2017) "Chaotic Visual Cryptography Based Digitized Document Authentication", Wireless Personal Communications, Vol.96, No. 3, pp. 3585–3605.
[31] Gelar Budiman and Ledya Novamizanti (2015) "White Space Steganography On Text By Using Lzw-Huffman Double Compression", International Journal of Computer Networks & Communications (IJCNC), Vol.7, No.2, pp. 123-136, DOI: 10.5121/ijcnc.2015.7210.
[32] Saraireh, Saleh (2013) "A Secure Data Communication System Using Cryptography and Steganography (2013)", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, pp. 125-137.

AUTHORS

Ritesh Mukherjee is associated with C-DAC (Centre for Development of Advanced Computing), Kolkata, India as an Associate Director. He has 22 years of experience in software solution development in the area of large databases, data warehousing, Web technologies, Mobile Computing, etc. He has contributed to more than 15 projects, the release of 7 solutions and 3 products. He has 14 research papers in various journals, and conferences, 3 copyrights, 1 Indian, and 1 US patent.

Anirban Goswami is currently working as Asst. Professor and Asst. Registrar in Techno India (An Engineering College under the Maulana Abul Kalam Azad University of Technology), Kolkata, West Bengal, India. He has more than 22 years of teaching experience He had contributed in more to 10 graduate-level projects and has 15 international conferences and 6 international journal publications. He did his Ph. D. from the Faculty of Engineering, Technology & Management, University of Kalyani.

Soumit Chowdhury is presently working as an Assistant Professor of Computer Science & Engineering, in the Govt. College of Engineering & Ceramic Technology, Kolkata, India. He has more than 16 years of teaching experience in different engineering colleges and has published 18 research papers in different National, International Journals and Conferences. He has also successfully supervised one UGC-funded research project as a Principal Investigator and did his Ph. D. in Engineering from the University of Kalyani.

Nabin Ghoshal is currently attached with the Department of Engineering & Technological Studies, University of Kalyani, Kalyani, West Bengal. He is sincerely involved with Teaching and Research work. His research areas are Steganography, Watermarking, Security, Bio-metric steganography, Visual Cryptography, Visual Cryptography through Steganography, Copyright protection, and authentication (Audio & Video). He received his Ph. D. in Computer Science & Engineering from the University of Kalyani in 2011. Dr. Ghoshal has 55 research papers in various international journals and national and international conferences. He wrote a book in his research area.
Dr. Ghoshal attended many national and international conferences in India and abroad.