EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

An Efficient DCT-SVD Steganographic Approach Applied to JPEG Images

Franklin Tchakounté[1,*], Priva Chassem Kamdem[1], Jean Claude Kamgang[2], Hortense Boudjou Tchapgnouo [3], Marcellin Atemkeng[4]

[1]Mathematics and Computer Science, Faculty of Science, University of Ngaoundéré, Cameroon
[2]Department of Mathematics and Computer Science , National School of Agro-Industrial Science, University of Ngaoundéré, Cameroon
[3]Department of Computer Science and Telecommunications, National School of Polytechnic of Maraoua, University of Maroua, Cameroon
[4]Department of Mathematics, Rhodes University, 6140 Grahamstown, South Africa

Abstract

To prove the origin of images in social media, this work proposes an efficient JPEG image steganography approach. After structuring the cover image into blocks of 8*8 pixels, Discrete Cosine Transform is applied to each block of pixels. The latter are quantified using a quantization table and a matrix of DC coefficients from quantized blocks of pixels, is obtained. Singular Value Decomposition is applied to the previous matrix and the secret message is inserted within singular vectors. For extraction purposes, previous transformations are followed reversely. An experimentation is made on seven images and results show that the proposed system outperforms similar studies in three aspects (i) it preserves stego image quality with PSNR of stego images varying between 38 and 54 (ii) it is able to insert a secret message of 257600 bits with the capacity of 4 bits per pixel (iii) it is robust and resistant to attacks such as histogram analysis and chi-square test.

Received on 19 June 2020; accepted on 22 September 2020; published on 28 September 2020

Keywords: Image steganography, JPEG, Discrete Cosine Transform, Insertion, Singular Value Decomposition, Quantization, Attacks, Social media

doi:10.4108/eai.28-9-2020.166365

1. Introduction

Social media gain a large audience since they provide means of instant communication of various types of information [1]. The proportion of social media users increased by 10 percent between 2019 and 2020, with 49 % of the global Internet population active on social media [2]. However, this popularity makes it a place for malicious people enticed to misinform and deceive people [3–6]. They refer to social engineering techniques and illegal means to compromise information. A major concern is therefore to verify information. Three trends are declined for this concern [7]. The first trend exploits cryptographic algorithms to keep integrity of original information by exploiting digital signatures [8], [9]. The second trend refers to the use of tattoo which protects the copyright of information by inserting a signature in the original information [10]. This signature is not directly visible without appropriate technique. The use of cryptography, on the other hand, is visible because there is a transformation of the original information into encrypted data. Steganography is the third trend. It is the art of hiding secret messages in cover medium such as image file, text file, video file, or audio file [11]. Steganography is used to mitigate the problem of transparency related to cryptography and tattooing techniques. Image is the most popular medium due to its high capacity and availability in the Web [12]. Image steganography is therefore a good candidate for verification of image and its evaluation criteria are quality of the transformed image (i.e. stego image), capacity bounds to insert the message and robustness to attacks such as histogram analysis and attack of χ^2.

*Corresponding author. Email: tchafros@gmail.com

Several studies have shown that image steganography ensures integrity and confidentiality but is not resistant to statistical attacks [8], [9], [13]. This work investigates specifically Joint Photographics Experts Group (JPEG) because (i) it is the popular image format in the web [14] and (2) it performs better concerning security compared to all other image formats [15] has good compression characteristics resistant to attacks. Image steganography related to JPEG provide good robustness but to the detriment of the quality of the image stego and insertion capacity [16], [17], [18], [19], [20], [21]. Following these limitations, the aim of this paper is to provide a steganographic system for JPEG images based on SVD insertion to simultaneously guarantee image quality, insertion capacity and robustness to attacks. Since the image steganography approach proposed by Sari et al. [22] fulfills the three criteria, but on various images, we exploit it to adapt to JPEG requirements. Our work makes two main contributions:

- We propose a JPEG image steganographic system by adapting the sari et al's work [22] to JPEG. Sari et al. 's work is efficient in terms of capacity, quality and robustness to basic attacks related to image processing. However, the Sari et al's proposal is not adapted to JPEG architecture. Our approach mimics this work by adapting to JPEG format while maintaining performance criteria.
- We perform experiments on seven well-known images and compare with similar approaches to evaluate the final system in terms of image quality, insertion capacity, and robustness. Results reveal that our approach is efficient in quality, insertion capacity and is robust to statistical attacks such as the χ^2 test and the histogram analysis.

The rest of the paper is organized in four sections. Section 2 presents works which are related to JPEG image steganography and which are exploited in this work. Section 3 proposes an approach of image steganography for JPEG images. Section 4 concerns implementation, results and discussions. In this section, criteria such as image quality, insertion capacity and robustness and comparison to similar approaches are made. The document ends with a conclusion and perspectives for further investigations.

2. Background

In this section, we describe the SVD technique and we present several studies, which deal with JPEG image steganography.

2.1. SVD technique

Loukhaoukha and Chouinard [23] indicated that the SVD foundations were settled for real square matrices in the 1870s by Beltrami and Jordan, for complex matrices by Autonne in 1902, and for rectangular matrices by Eckart and Young in the 1939. SVD has been adopted in image processing applications such as image compression, image hiding, and noise reduction [24]. It is often very difficult to extract, from a matrix, features of interest to solve a given problem [25] [26]. An effective method is to highlight the matrix properties and to factorize that matrix as a scalar of simpler matrices with more structured characteristics. Then, the secret message is dissected and inserted into singular vectors. This process resists attacks which directly analyze images.

Principle of SVD. We consider a real or complex matrix M of size $m \times n$ and of rank r. Then, an orthogonal matrix U of size $m \times m$, an orthogonal matrix V of size $n \times n$ and a rectangular matrix S of dimension $m \times n$, exist. Formally, the decomposition into singular values of M is the factorization given in Equation 1 [26].

$$M = USV^T \tag{1}$$

$$\begin{cases} UU^T = I(m) \\ VV^T = I(n) \\ S(m,n) = \begin{pmatrix} s_1 & 0 & ... & 0 & 0 \\ 0 & s_2 & ... & 0 & 0 \\ 0 & 0 & . & 0 & 0 \\ 0 & 0 & 0 & & s_n \end{pmatrix}. \end{cases}$$

$s_1, s_2 \ldots s_n$ are the singular values of the matrix M. These values are positive real numbers, which respect the following condition:$s_1 > s_2 > s_3 > \ldots . > s_n$ [26].

Advantages of SVD in steganography. The use of SVD in steganography is motivated by the following arguments [25] [27].

- The singular values represent the energy of the image, i.e. SVD arranges the maximum of energy of the image in a minimum of singular values;
- A good stability is provided by the singular values of an image, i.e., when a small disturbance (a mark or a signature) is inserted in an image, the singular values do not change significantly . It offers robustness against common signal attacks and image processing attacks;
- Factorization in SVD is unique.

2.2. JPEG image steganography

Several JPEG image steganography approaches has been proposed [16], [17], [18], [19], [20], [21]. These approaches are briefly reviewed in this section. JSteg was the first steganography system designed for images compressed in JPEG format [20]. During the integration process, JSteg integrates sequentially the secret message

bits into the least significant bits (LSB) of certain DCT coefficients quantized and selected based on the zigzag scanning order. JSteg is not suitable for withstanding attacks from the chi-square χ^2 family because LSB is used to integrate the secret message. To increase the number of non-zero quantified DCT coefficients, Chang et al. [16] use a modified quantization table when compressing images based on JPEG. Their approach is also not suitable for chi-square attacks because they rely on LSB substitution to integrate the secret message bits sequentially into the quantized DCT coefficients. OutGuess [19] includes another process of insertion. This process integrates non-sequentially the bits of the secret message by replacing the LSB bits of the quantized DCT coefficients. With this process, OutGuess is able to avoid chi-square attacks. The three previous proposals have in common that they are all based on direct modification of the quantized DCT coefficients using LSB substitution methods for the integration of secret message bits. Due to the fact that LSB is vulnerable, other substitution methods for inserting the bits of the secret message are employed. The F5 algorithm [21] implements a matrix encoding which improves insertion capacity and provides better security at the same time. F5 algorithm uses matrix encoding and permuted overlap to encode the bits of the message. Although F5 is secure against most statistical attacks like histogram attack, χ^2 attack, it suffers from the narrowing effect and that the receiver cannot distinguish a coefficient of zero value, whether it is steganographically unused or produced due to the modification of absolute values of 1 and -1. Liu et al. [17] proposes a complementary insertion scheme to integrate the secret message into the quantified DCT coefficients. This scheme overcomes the narrowing effect and is able to resist various attacks by steganalysis. All the previous JPEG-based steganographic schemes have the common limitation that one single bit of the secret message can be integrated into each authorized quantized DCT coefficient. So the insertion capacity is 1 bit. Pal et al. [18] proposes a JPEG based steganography scheme able to integrate two bits of secret message through each allowed quantized DCT coefficients and able to resist against some steganographic attacks. Similarly, Chang et al. [16] allow insertion of secret message with pixels of two bits but providing low image quality.

None of JPEG based steganography schemes fulfills simultaneously high embedding capacity, image quality and resistance to attacks such as the χ^2 and histogram analysis. The aim of this paper is to propose an attempt to overcome this limitation. Watermarking techniques can offer these properties [28]. We are interested in the Sari et al.'s work which offers this fulfillment capability. We propose further a JPEG image steganography scheme by mimicking the Sari et al's insertion of secret message. This proposal is able to provide a 4-bit embedding capacity while preserving quality of image and robustness against attacks.

3. Proposed approach

In this section, the proposed approach of JPEG image steganography is described. This approach includes two modules as shown in Figure 1. The first module is responsible to encode and hide the secret message and the second module is responsible to extract and decode the hidden message. The insertion and extraction of the secret message relies on DCT and SVD. The first module is broken down into five layers. The first layer aims to transform the image into blocks of 8 * 8 pixels. The second layer is responsible for DCT transformation. This layer decorrelates blocks of pixels from the input image. The third layer is responsible for quantization. In this layer, the blocks of pixels decorrelated in the previous layer are quantified. The fourth layer concerns the insertion phase of the secret message. In this layer, the secret message is inserted within the cover image. The fifth layer refers to entropy encoding. In this layer, data are compressed to finally generate the JPEG image file. The second module also has five layers but each layer performs reverse operations of the corresponding layer in the first module. The following sections provide technical details of each layer in the first module.

3.1. Structuring in 8 × 8 blocks of pixels

In this layer, the image taken as input is subdivided into 8 × 8 blocks on which the following layers perform independently. When the width and the length of that image are not multiples of 8, we add columns by repeating the last until reaching a multiple of 8. The principle is the same concerning lines.

This breakdown is due to the following reasons. Applying DCT to all N × N pixels of an image requires cutting because it allows data units to reduce the compression rate and faster.

Correlations between pixels of an image are of short range. Each pixel has a value that is close to its neighbors, but has nothing to do with the values of distant neighbors.

3.2. DCT transformation

DCT is one of the most common transformation techniques in image compression (A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine). DCT is the basis of transformation used in the JPEG standard (Image compression using DCT upon various quantization). DCT is applied to each block of 8x8 pixels obtained in the first layer and provides new blocks of 8x8 pixels. The result provided is represented in a matrix

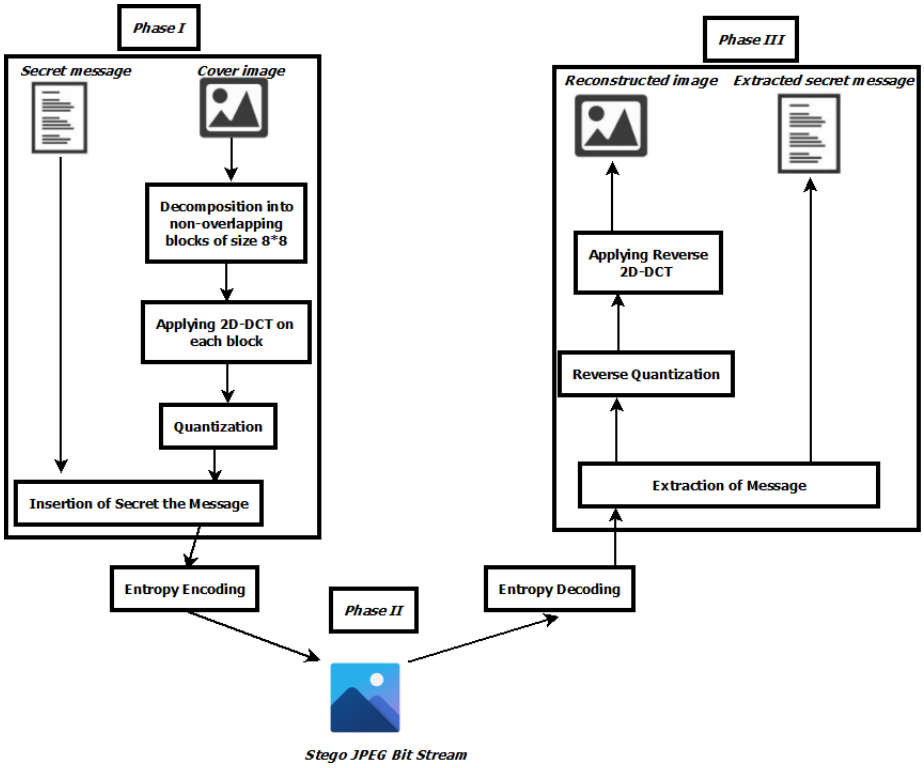

Figure 1: Architecture of the proposed approach

of the same dimension. The energy in the transformed coefficients is concentrated on the upper corner of the coefficient matrix. The low frequencies at the top left of the matrix, and the high frequencies at the bottom right. DCT is calculated on a matrix of N x N as given in Equation 2.

$$DCT(i,j) = \frac{2}{N}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}pixel(x,y) \cos[\frac{(2x+1)i\pi}{2N}]\cos[\frac{(2y+1)j\pi}{2N}] \quad (2)$$

where:

- DCT (i,j) represents the value of the DCT at the point of coordinates (i, j) in the block of 8x8 pixels.
- Pixel (x, y) represents the value of the pixel of coordinates (x, y) in the block of the original image of 8x8 pixels.

The DCT coefficients include the DC coefficient and the AC coefficients. The DC coefficient is the coefficient which has zero frequency in both dimensions whereas the AC coefficients are the 63 others having non-zero frequencies. Most of the spatial frequencies have zero or near-zero amplitude and not need to be encoded.

Since the DCT matrix transformation is an orthogonal transformation, it is associated with an inversion method to be able to extract the secret message within the JPEG file from the stego image. The inverse DCT on each of the 8x8 blocks is defined in Equation 3.

$$pixel(x,y) = \frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(i)C(j)DCT(i,j)cos[\frac{(2x+1)i\pi}{2N}] cos[\frac{(2y+1)j\pi}{2N}] \quad (3)$$

$$C(x) = \frac{1}{\sqrt{2}} \qquad if\ x\ holds\ 0,\ and\ 1\ otherwise\ . \quad (4)$$

3.3. Quantification

Quantification follows the DCT transformation. Here, the DCT blocks obtained from the upper layer are quantified. Each element of the upper layer's matrix is divided by its corresponding element in the quantification matrix. The quantification matrix characterizes the sensitivity of the eye in each frequency zone. This matrix is therefore rounded down to the nearest whole number after dividing by the coefficient of quantification. For a block F of the matrix's image, its quantization is expressed as in Equation 5.

$$F'(x,y) = \frac{F(x,y)}{Q(x,y)}. \quad (5)$$

Where Q represents the quantification matrix. The reverse quantization is represented in Equation 6.

$$F(x,y) = F(x,y) \times Q(x,y) \tag{6}$$

In the proposed scheme, the quantification table is the modified quantification table defined in [29]. This table is significantly different from the standard JPEG quantization table. The modified quantification matrix has the following advantages:

- It improves the capacity of insertion or concealment within the original image [30]. This table allows us to hide more data.
- This table also allows the stego image to limit distortions visible to the human eye.

$$Q = \begin{bmatrix} 8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 14 \\ 1 & 1 & 1 & 1 & 1 & 1 & 14 & 15 \\ 1 & 1 & 1 & 1 & 1 & 14 & 15 & 16 \\ 1 & 1 & 1 & 1 & 14 & 15 & 16 & 18 \\ 1 & 1 & 1 & 14 & 15 & 16 & 18 & 20 \\ 1 & 1 & 14 & 15 & 16 & 18 & 20 & 22 \\ 1 & 14 & 15 & 16 & 18 & 20 & 22 & 23 \end{bmatrix} \tag{7}$$

In case the quantization operation is performed correctly, two situations occur. Very few zeros appear on the left of the DCT coefficient matrix (blocks of pixel) and information in the matrix is typically concentrated in the upper left region of blocks of pixels.

3.4. Insertion of secret message

In this layer, the process of concealing the secret message in the image is performed. Figure 2 depicts this process.

The DCT blocks of pixels are divided into DC coefficient and AC coefficients. In the matrix's image, the DC coefficients of each sub-block (blocks of pixels) are gathered to obtain the DC coefficient matrix.

The DC matrix is composed of only DC coefficients of blocks of pixels of the image matrix. The size of the matrix of DC coefficient is $[N/8] \times [M/8]$ when the image matrix is of size $N \times M$. The SVD technique is then applied to the matrix of DC coefficients. The expression in the form $U * S * V$ is exploited after transformations. The process of insertion is the resumption of the principle of insertion proposed by Sari et al. [22]. It has two advantages: (i) good performance and (ii) the DC coefficients selected as the place for insertion, are useful and robust against various attacks. The principle of integration is as follows:

$$S' = S + \alpha L_m \tag{8}$$

Where

- S' is the singular value after insertion;
- S is the singular value of the DC matrix;
- α is the intensity factor of the insertion;
- L_m is the secret message.

After the insertion, reverse SVD is applied on matrices U, S' and V using the formula $U * S' * V^T$. This formula provides the reverse of SVD transformation where V^T is the transpose of the orthogonal matrix V. The inverse of SVD is helpful to reconstruct the matrix of DC coefficients.

The next step consists to reconstruct the blocks of pixels with their DC coefficients. These numbers represent the JPEG output, but they are compressed before being included in the output file. This phase is called entropy encoding and is described in the next section.

Algorithm 1: Insertion algorithm

Result: JPEG file of the stego image
Input: cover image, secret message;
Decomposed into non-overlapping blocks of size 8×8;
Applying 2D-DCT on each block;
Applying Quantification;
Collecting DC coefficients on each block;
$M'_{DC} = \text{SVD}(M_{DC})$;
msg = 1;
while $msg \neq message_{size}$ **do**
  $S'_i = S_i + \alpha L_{mi}$;
  msg = msg +1
end
$M'_{DC} = U * S' * V^T$;
Reconstruction of each block with DC coefficient;
Entropy encoding;

3.5. Entropy encoding

This layer is dedicated to the process of encoding DC coefficients. This process aims at compressing the data before writing it to an output file. Entropy encoding, illustrated in Figure 4, involves encoding symbols that have a high probability of occurrence with shorter words than symbols that have a low probability of occurrence. However, the DC coefficient of the pixel block and the other 63 DC coefficients are coded separately.

DC coefficients are coded in DPCM (Differential Pulse Code Modulation) using the DC value of the DC coefficient from the previous block as presented in Equation 9.

$$DIFF = DC_i - DC_{i-1} \tag{9}$$

The goal of this process is to exploit the correlation between the DC values of adjacent blocks and to encode

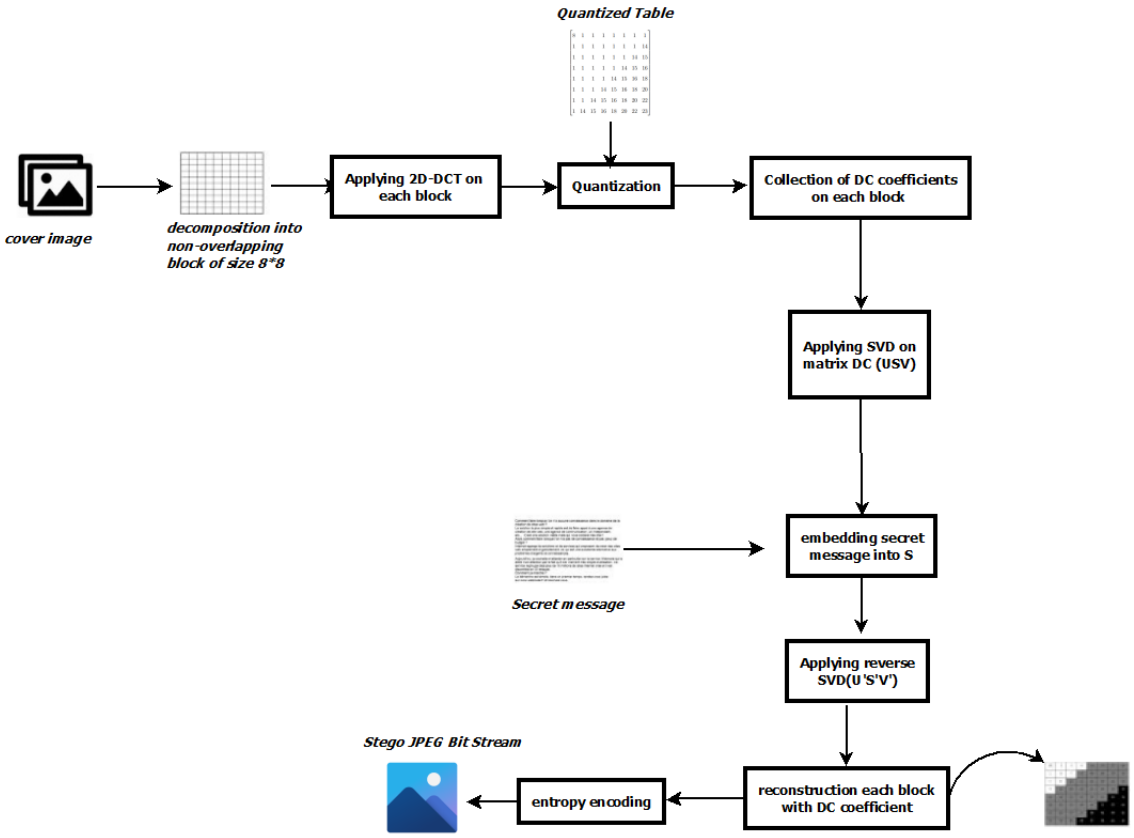

Figure 2: Insertion process

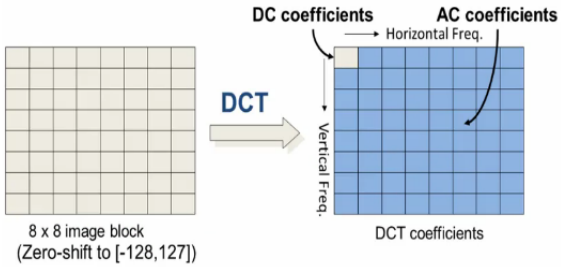

Figure 3: An illustration of DCT block of pixels [31]

them more efficiently. These blocks typically contain most of the image energy. The other 63 AC coefficients starting from AC (0,1) are range coded after a Zigzag scan as shown in Figure 5.

The purpose of Zigzag scanning is to facilitate entropy coding by first encountering the coefficients most likely to be non-zero or the low frequency coefficients. The JPEG algorithm employs a combination of RLE(Run Length Encoding) and Huffman or arithmetic encoding. The idea is that the sequence of AC coefficients contains just a few non-zero numbers, with the number zero between them.

3.6. Extraction

Now, the extraction process is described. The aim in this process is to extract a secret message from the stego file. This process is depicted in Figure 7.

In our approach, the extraction model takes the JPEG file of the stego image as input and returns the hidden message. It is realized in different stages. The first stage concerns entropy decoding of the JPEG compressed image. The second stage concerns extraction of the message concealed in the stego file. The third stage concerns the inverse quantization and the reverse DCT to reconstruct the original image.

Algorithm 2: Algorithm of extraction

Result: secret message
Input: JPEG file of the stego image ;
    Reading the JPEG image file;
    Entropy decoding of the stego image;
    Collecting the DC coefficients and determining the matrix M_{DC};
    $M'_{DC} = \text{SVD}(M_{DC})$;
    msg = 1;
while $msg \neq message_{size}$ **do**
    $L_{mi} = (S'_i - S_i)/\alpha$;
    msg = msg + 1
end

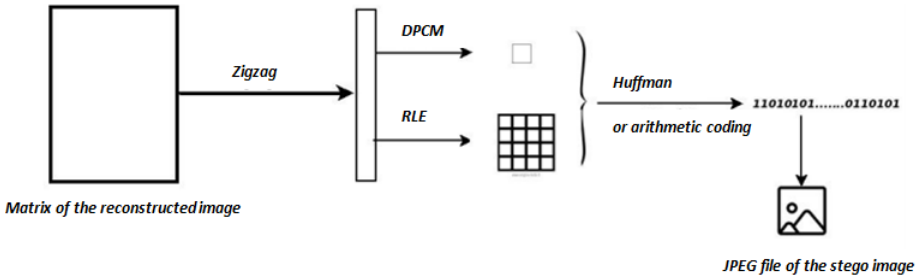

Figure 4: Entropy encoding

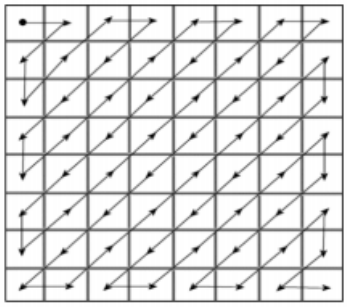

Figure 5: Zigzag scanning

3.7. Experimentation and discussions

Experiments are realized on a dataset of seven grayscale images available in literature [18]. They all are 512 x 512 as presented in Figure 8.

In the following, results with this dataset are presented and discussed. The performance of the steganography system is assessed in terms of quality of the stego image, insertion capacity and robustness.

The stego image is obtained after performing layers in the first module of the proposed approach. The secret message is inserted in the cover image by modifying the transformed and quantized coefficients (DCT) of the cover medium and these coefficients are further encoded by appropriate entropy encoding to obtain all the compressed data. The compressed data set is considered as a compressed version of the stego image from which the receiver can extract the secret message. The first assessment criteria is fulfilled when the receiver has a good visual or high quality image after the decompression process. Figure 9 illustrates reconstructed images.

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are computed to assess the level of visual quality of stego images [32]. MSE is the cumulative squared error between the compressed and the original image. It is recommended to have lower the value of MSE because it indicates that both images are nearly similar. PSNR is a ration, which measures the quality between the original and a compressed image. The higher the value of PSNR, the better the quality of the compressed or the reconstructed image. MSE is given in Equation 10.

$$MSE = \frac{\sum_{M,N}[IMG_1(M,N) - IMG_2(M,N)]^2}{M \times N} \quad (10)$$

where IMG_1 is the original image and IMG_2 is the compressed image. M is the number of rows and N is the number of columns. PSNR is given in Equation 11.

$$PSNR = 10log_{10}(\frac{R^2}{MSE}) \quad (11)$$

where R is the maximum fluctuation in the input image data type. MSE is the mean-square error.

Results about image quality are presented in table 1. We see that PSNR of stego images varies between 38 and 54 which shows that the proposed approach presents very good results in terms of image quality. The following images: boat, goldhill are better reconstructed after applying the proposed steganography system since they have the lowest MSE and the highest PSNR. Our approach is able to provide better PSNR and MSE at the same time. This capability means that even if the secret message is inserted, the stego image is not as different as the original image. Therefore, the image can be propagated without any visible alteration. It can be reconstructed and verified through the system.

As we compare our approach to similar works in table 2 based on PSNR, we find that our proposed approach reaches the highest values of PSNR. This result presents the dominance of our approach. In conclusion, our system outperforms the others in terms of visual quality of the stego images.

The second important concern in steganography is the capacity to insert secret messages without distorting the quality of the stego image, so that the stego image is almost identical to the cover support. Table 3 presents a comparison of our approach to similar works in terms of insertion capacity. Our approach provides a value

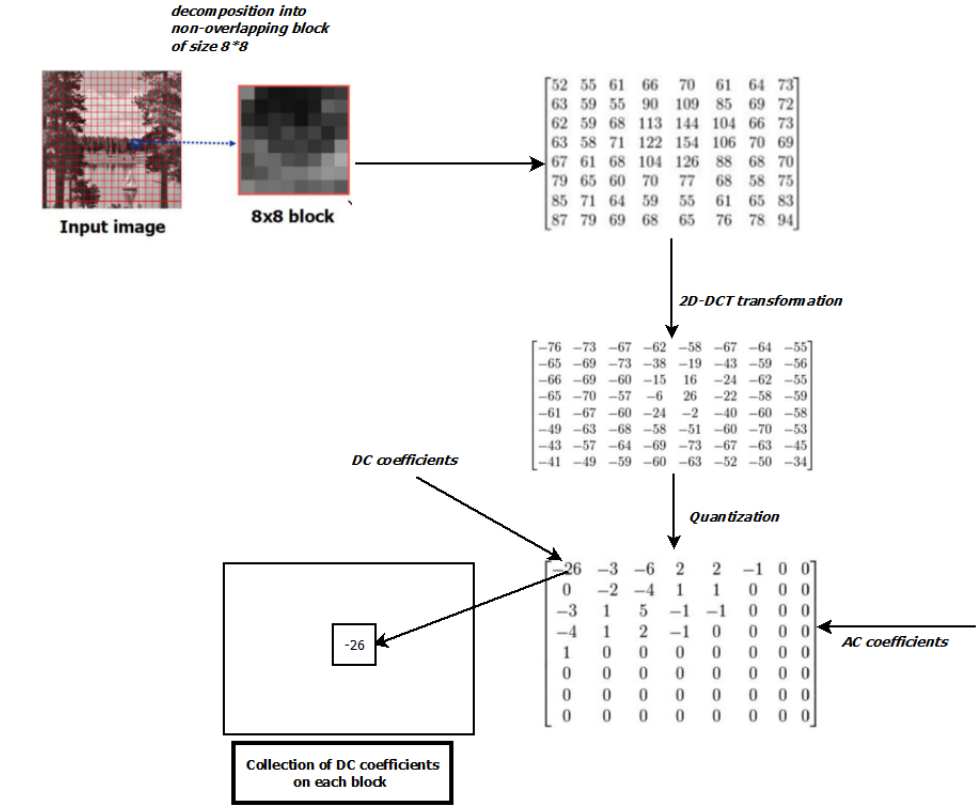

Figure 6: Principle of insertion

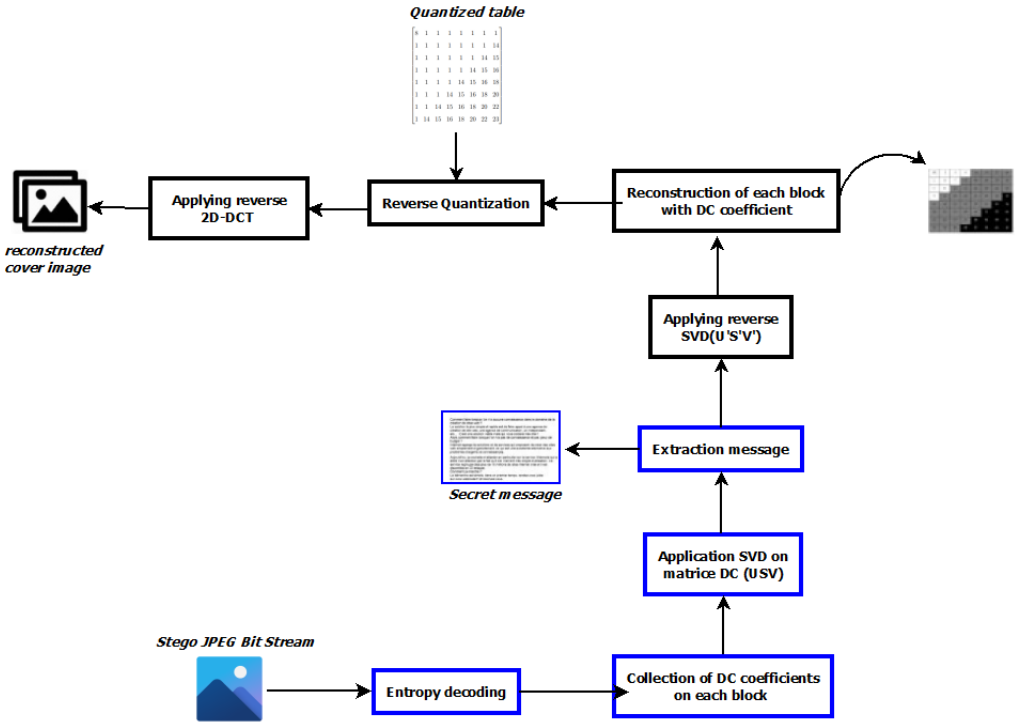

Figure 7: Extraction principle

257600 bits, which is the maximum size of the message to be inserted. This value is the highest compared to the others.

Figure 8: Samples

Figure 9: Stego images

Table 1: Assessment of visual quality

Images	lena	pepper	boat	barbara	goldhill	zelda	mandrill
MSE	3.4574	6.1459	0.33	4.0008	0.20	2.8059	0.5812
PSNR	42.63	40.14	52.94	42.1093	54.9881	43.65	38.69

The third criteria required to assess a steganographic system is the resilience to attacks. The robustness of our system against histogram analysis and χ^2 attacks is analyzed. Concerning the histogram analysis attack, the aim is to show that there is no difference between the histogram of original image and the histogram of the stego image [18]. If there are variances, the system is not resilient to this attack. The histogram of the stego image

Table 2: Our approach vs. similar works in terms of PSNR

Images/Approach	JSteg [20]	F5 [21]	OutGuess [19]	Chang et al. [16]	Li and Liao [17]	Pal et al. [18]	Our approach
Lena	36,36	36,94	36,37	33,84	35,67	39,09	42,63
Peppers	35,45	35,86	35,32	32,98	34,75	37,59	40,14
Boat	35,67	36,13	35,47	33,29	34,53	38,74	52,94
Barbara	32,51	32,83	32,10	31,13	26,41	34,27	42,10
Goldhill	33,02	35,40	35,12	31,78	33,03	37,17	54.98
Zelda	38,31	38,32	38,22	36,45	37,64	40,86	43.65
Mandrill	27,86	28,13	27,89	27,63	23,25	30,10	38,69
Average	34,148	34,8014	34,3557	32,4428	32,1828	36,831	45,02

Table 3: Our approach vs. similar works in terms of insertion capacity (in bits)

Images/Works	JSteg [20]	F5 [21]	OutGuess [19]	Chang et al. [16]	Li and Liao [17]	Pal et al. [18]	Our approach
Lena	32998	33026	16375	104578	44131	104578	257600
Peppers	45363	45513	22699	105600	59229	105600	257600
Boat	38374	38506	19105	105578	50042	105578	257600
Barbara	45363	45513	22699	105600	59229	105600	257600
Goldhill	45196	45505	22639	125176	60890	125176	257600
Zelda	27557	27630	13724	89514	37086	89514	257600
Mandrill	75751	75837	37867	152302	98989	²152302	257600

is constructed by plotting quantified DCT coefficients from the stego file in order to expose the histogram. The histogram of the original image is directly generated from its pixels.

Figure 11 and 14 represent respectively the histogram of the cover image and the histogram of the stego image. We realized that there is no variations. We realize the same on two research works as shown in Figure 12 and in Figure 13 : [18] and [17]. But these works have been applied only on the reconstructed images from JPEG bit streams.

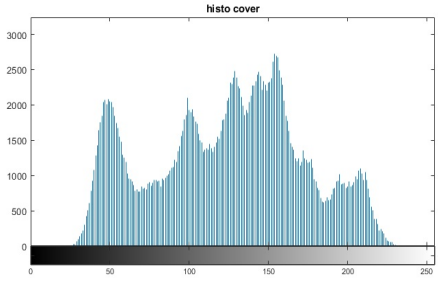

Figure 10: Cover image

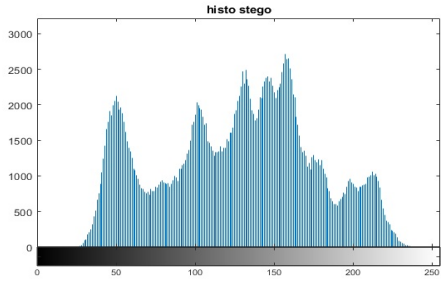

Figure 11: Stego image in our approach

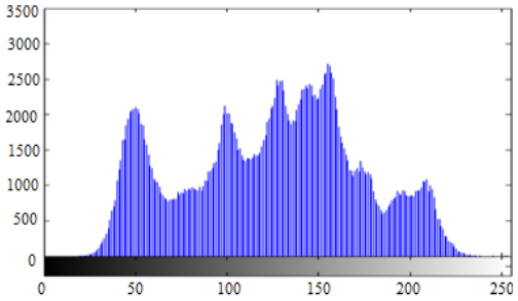

Figure 12: Approach in [18]

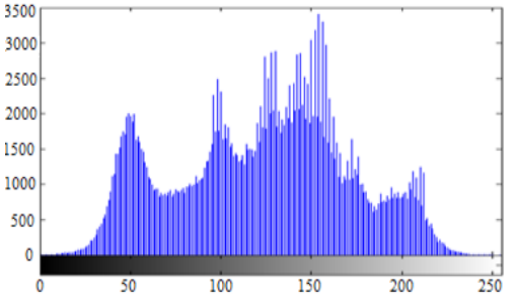

Figure 13: Approach in [17]

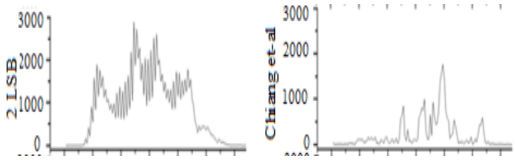

Figure 14: D_k for LSB and [18]

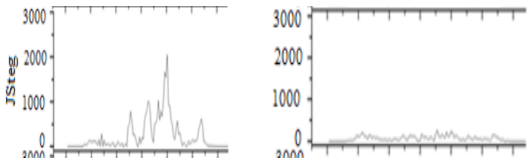

Figure 15: D_k for [20] and [18]

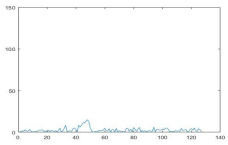

Figure 16: D_k for our approach

We also observe that [18] is resilient to histogram analysis since there is almost no variation between the stego and the original cover image. Unlike, Liu and Liao's histogram indicates distortions on the stego image. So this work is susceptible to the histogram analysis attack.

The χ^2 attack holds generally in LSB. This attack detects the existence of the hidden message based on the variation of pair of values (PoVs) in the stego image. The variation of PoVs for any image is identified as follows [18]. We consider that X_k and Y_k are frequency occurrences for pixels 2k and 2k + 1 respectively, for k = 0, 1, 2, ..., 127. Now, D_k is the difference of pixels 2k and 2k + 1 of any image, and its formula is given in Equation 12.

$$D_k = abs(X_k - Y_k)[18] \tag{12}$$

where abs (.) represents the absolute function.
Histograms with values of D_k are plotted in Figures 14, 15, and 16 only for the Lena image. Figure 14 illustrates D_k values for LSB and [16]. Figure 15 illustrates D_k values for [18] and [20]. Figure 16 depicts D_k values of the stego image using our approach.

Results show that variations of D_k are very small in our approach and [18]. It is visible since curves are near the abscissa axis. The proposed approach is resilient to the χ^2 test attack since it is based on SVD insertion, which is a technique that offers robustness against common attacks [25]. LSB looks to be the most vulnerable regarding its curve. Indeed, D_k points points move away from the abscissa axis. Likewise, approaches in [16] and [20] present bad results in terms of D_k.
Concerning robustness, experiments reveal that our approach is resistant to statistical attacks such as the χ^2 test and histogram analysis.
Table summarizes other works taken from the literature, which are evaluated according to criteria defining the performance of a steganographic system. From this table we can therefore say that the proposed approach improves previous works in particular the study [18].

Simulations and development of system have been made on MATLAB R2018a (9.4.0.813654) 64bits. MATLAB has been used because this scientific environment provides intensive in-built image processing modules. Compared to similar works, the proposed JPEG image steganography provides better results in terms of image quality, insertion capacity and resilience to attacks such as χ^2 test and histogram analysis. This approach takes

Table 4: Our approach vs. similar works in terms of robustness. ∨ = yes and × = no

Approaches/Criteria	Quality (psnr>35db)	Capacity (in bits) by coefficient	Resistance to χ^2	Resistance to histogram
JSteg [20]	×	1	×	×
OUTGUESS [19]	×	$\frac{1}{2}$	∨	∨
F5 [21]	×	1	∨	∨
Chang et al. [16]	×	2	×	×
Liu et liao [17]	×	1	∨	∨
Pal et al. [18]	∨	2	∨	∨
Our system	∨	4	∨	∨

advantage of SVD insertion of a robust image steganography system. These results demonstrate that it is possible to exploit image steganography methodologies to improve JPEG image steganography. However, our system should be tested against more recent attacks such as reverse JPEG compatibility [33].

4. Conclusion and perspectives

The aim of this work was to propose a JPEG steganography approach that simultaneously guarantees image quality, insertion capacity and robustness to attacks. For that, an approach of insertion of secret text has been designed and implemented with the particularity of adapting the Sari et al. [22]' s embedding approach to JPEG.

The experiments performed on seven images revealed that the proposed system (i) is efficient concerning quality of stego image (ii) is able to take 4 bits per pixel for insertion of message (iii) is robust and resistant to attacks such as histogram analysis and attack of χ^2. A comparison with similar JPEG steganography approaches revealed that the proposed approach provides better properties.

Future works include two main directions. The first direction is to investigate other image steganography approaches that we can exploit to improve performance of the proposed system. The second direction is to reinforce our system to recent attacks.

References

[1] S. A. Asongu and N. M. Odhiambo, "Governance and social media in African countries: An empirical investigation," *Telecommunications Policy*, vol. 43, pp. 411–425, jun 2019.

[2] D. Chaffey, "Global social media research summary 2020," apr 2020.

[3] H. Almarabeh and A. Sulieman, "The impact of cyber threats on social networking sites," *International Journal of Advanced Research in Computer Science*, vol. 10, no. 2, p. 1, 2019.

[4] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.

[5] F. Tchakounté, A. Faissal, M. Atemkeng, and A. Ntyam, "A reliable weighting scheme for the aggregation of crowd intelligence to detect fake news," *Information (Switzerland)*, vol. 11, no. 6, 2020.

[6] F. Tchakounté, C. K. Amadou, A. A. Abba Ari, and D. J. Fotsa Mbogne, "A smart contract logic to reduce hoax propagation across social media," *Journal of King Saud University - Computer and Information Sciences*, sep 2020.

[7] R. Ruchi and U. Ghanekar, "A Brief Review on Image Steganography Techniques ," in *International Conference on Advances in Electronics, Electrical & Computational Intelligence (ICAEEC)*, (IIIT Allahabad India), 2019.

[8] D. N. Aini, S. N. Putro, E. H. Rachmawanto, C. A. Sari, *et al.*, "Survey of methods in the spatial domain image steganography based imperceptibility and payload capacity," in *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, pp. 434–439, IEEE, 2019.

[9] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, "Achieving data integrity and confidentiality using image steganography and hashing techniques," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, pp. 1–6, IEEE, 2019.

[10] X. Di and V. M. Patel, "Deep learning for tattoo recognition," in *Advances in Computer Vision and Pattern Recognition*, vol. PartF1, pp. 241–256, Springer London, 2017.

[11] K. H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing," *Imaging Science Journal*, vol. 63, pp. 398–407, sep 2015.

[12] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 313–335, 1996.

[13] A. Nikishova, M. Y. Umnitsyn, and T. Omelchenko, "Hidden data transmission during organizations interaction," in *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, pp. 1–5, IEEE, 2019.

[14] A. Cohen, N. Nissim, and Y. Elovici, "MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images," *IEEE Access*, vol. 8, pp. 19997–20011, 2020.

[15] A. S. Ansari, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats ," *International Journal of Computer Network and Information Security*, vol. 1, pp. 11–25, 2019.

[16] C.-C. Chang, T.-S. Chen, and L.-Z. Chung, "A steganographic method based upon jpeg and quantization table modification," *Information Sciences*, vol. 141, no. 1-2, pp. 123–138, 2002.

[17] C.-L. Liu and S.-R. Liao, "High-performance jpeg steganography using complementary embedding strategy," *Pattern Recognition*, vol. 41, no. 9, pp. 2945–2955, 2008.

[18] A. K. Pal, K. Naik, and R. Agrawal, "A steganography scheme on jpeg compressed cover image with high embedding capacity.," *Int. Arab J. Inf. Technol.*, vol. 16, no. 1, pp. 116–124, 2019.

[19] N. Provos, "Defending against statistical steganalysis.," in *Usenix security symposium*, vol. 10, pp. 323–336, 2001.

[20] D. Upham, "Jsteg steganographic algorithm," *Available on the internet ftp://ftp. funet. fi/pub/crypt/steganography*, 1999.

[21] A. Westfeld, "F5—a steganographic algorithm," in *International workshop on information hiding*, pp. 289–302, Springer, 2001.

[22] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by dc coefficients using singular value decomposition," in *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, pp. 1–5, IEEE, 2017.

[23] K. Loukhaoukha, "Security of ownership watermarking of digital images based on singular value decomposition," *Journal of Electronic Imaging*, vol. 19, p. 013007, jan 2010.

[24] R. K. Singh and A. K. Singh, "A Recent Survey of DCT Based Digital Image Watermarking Theories and Techniques: A Review," in *Communications in Computer and Information Science*, vol. 1075, pp. 431–440, Springer, jun 2019.

[25] V. I. Gorodetski, L. J. Popyack, V. Samoilov, and V. A. Skormin, "Svd-based approach to transparent embedding data into digital images," in *International Workshop on Mathematical Methods, Models, and Architectures for Network Security*, pp. 263–274, Springer, 2001.

[26] S. Singh, R. Singh, and T. J. Siddiqui, "Singular value decomposition based image steganography using integer wavelet transform," in *Advances in signal processing and intelligent recognition systems*, pp. 593–601, Springer, 2016.

[27] K. Hetatache, *Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformées discrètes*. PhD thesis, 2018.

[28] A. Menendez-Ortiz, C. Feregrino-Uribe, R. Hasimoto-Beltran, and J. J. Garcia-Hernandez, "A Survey on Reversible Watermarking for Multimedia Content: A Robustness Overview," *IEEE Access*, vol. 7, pp. 132662–132681, 2019.

[29] S. Mitra, M. Dhar, A. Mondal, N. Saha, and R. Islam, "Dct based steganographic evaluation parameter analysis in frequency domain by using modified jpeg luminance quantization table," *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, pp. 2278–0661, 2015.

[30] V. K. Maan and H. S. Dhaliwal, "32× 32 vector quantization based colour image steganography," *International Journal of Enhanced Research in Science Technology & Engineering, ISSN*, pp. 2319–7463.

[31] Bogotobogo, "Digital Image Processing - Compression 2020," 2020.

[32] S. Krivenko, M. Zriakhov, V. Lukin, and B. Vozel, "MSE and PSNR prediction for ADCT coder applied to lossy image compression," in *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, pp. 613–618, Institute of Electrical and Electronics Engineers Inc., jul 2018.

[33] J. Butora and J. Fridrich, "Reverse JPEG Compatibility Attack," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1444–1454, 2020.