# Bitplanes Image Encryption/Decryption using Edge Map (SSPCE Method) and Arnold Transform

Ali Ukasha
Sebha University
Faculty of Engineering
Libya
elokshy@yahoo.com

***ABSTRACT:*** *Data security needed in data transmission, storage, and communication to ensure the security. The single step parallel contour extraction (SSPCE) method is used to create the edge map as a key image from the different Gray level/Binary image. Performing the X-OR operation between the key image and each bit plane of the original image for image pixel values change purpose. The Arnold transform used to changes the locations of image pixels as image scrambling process. Experiments have demonstrated that proposed algorithm can fully encrypt 2D Gary level image and completely reconstructed without any distortion. Also shown that the analyzed algorithm have extremely large security against some attacks like salt & pepper and JPEG compression. Its proof that the Gray level image can be protected with a higher security level. The presented method has easy hardware implementation and suitable for multimedia protection in real time applications such as wireless networks and mobile phone services.*

**Keywords:** SSPCE Method, Image Compression, Salt & Peppers Attacks, Bitplanes Decomposition, Arnold Transform, Lossless Image Encryption

**Received:** 17 February 2014, Revised 20 March 2014, Accepted 27 March 2014

## 1. Introduction

As we know various businesses require exchanging information in terms of text, images and videos over different communication channels; it is very necessary to protect that data from unintended users. From ancient time it is seen that encryption is the best way for protecting the data from unauthorized access. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to convert digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. Image security is a major challenge in storage and transmission applications. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. As we know images are the main source to attract the people [2], they are used in large scale in various fields like biometrics, military, medical science and online albums [3]. Interesting approaches for image encryption have been developed. They are designed to protect multimedia content and fulfill the security requirements for a particular multimedia called application such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) methods which incur large computational costs and show poor error resilience [4]. Therefore, it is important to guard images from illegal access and provide the security, integrity, confidentiality and reliability to it. Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain [4]. These approaches have extremely low security levels due to the lack of security keys. Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations [2]. This security method is also much lower because the results of its decomposition process and logic operations are predictable. It's not immune to plaintext attacks. To achieve higher levels of security, solution is to change image pixel values or blocks while scrambling the positions using different techniques. In this work we propose and evaluate selective bit plane encryption for confidential transmission of image data in mobile environments [3].

There are method is proposed for uncompressed image, which applies to a binary image, consist in mixing image data and a message (key) that has the same size as the image [1]: a XOR function is sufficient when the message is only used once. A generalization to gray level images is straightforward: Encrypt each bit plane separately and reconstruct gray level image. With this approach no distinction between bit planes is introduced although the subjective relevance of each bit plane is not equal. The highest bit planes exhibit some similarities with the gray level image, but the least significant bit planes look random. Because encrypted bits also look random, the encryption of least significant bit planes will add noise to the image. The advantage of least significant bits is that plaintext attacks are harder on random like data. It is preferable to encrypt bits that look most random.

## 2. Arnold Transform Map

The classical Arnold transformation converts any linear second order ordinary differential equation (LSODE) into the free Galilean particle equation [5]. Watermark must be encrypted before embedding into its carrier. It will go through scrambling transformation so that the spatial correlation of watermark image pixels will be cancelled and its security will be strengthened. In this way, attackers cannot accurately identify the specific content of watermark even if they already extract it. A binary image after digital processing can be viewed as a matrix, one pixel corresponding to one matrix element. After linear or nonlinear transformation of the pixels in the matrix, the image will look desultorily. A binary watermark image will look more like noise after being transformed several times, thus, attackers will take it as noise and ignore it even when they know the imbedding algorithm and already extract the embedded data. Therefore, the security of watermark is strengthened. There are many common ways to scramble watermark images as a pre-treatment such as Arnold transformation, magic transformation, Hilbert curve, Conway game, broad Gray code transformation, affine transformation and orthogonal Latin square transformation [6]. In this paper, we adopt a simple way but with strong security Arnold transformation. Arnold transformation also called cat face transformation. The Arnold transformation is defined as follows

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} ] \bmod (N) \qquad (1)$$

where $(x, y)$ and $(x', y')$ are the pixel coordinates of the original image and the encrypted image, respectively.

Let $\boldsymbol{A}$ denote the left matrix in the right part of equation (1), $\boldsymbol{I}(x, y)$ and $\boldsymbol{I}(x', y')^{(n)}$ represent pixels in the original image and the encrypted image obtained by performing Arnold transform $n$ times, respectively. Thus, image encryption using $n$ times Arnold transforms can be written as

$$\boldsymbol{I}(x', y')^{(k)} = A\,\boldsymbol{I}(x, y)^{(k-1)} (\bmod N) \qquad (2)$$

where $k = 1, 2, \ldots, n$, and $\boldsymbol{I}(x', y')^{(0)} = \boldsymbol{I}(x, y)$. Obviously, one can multiply the inverse matrix of $\boldsymbol{A}$ at each side of equation (2) to obtain $\boldsymbol{I}(x, y)^{(k-1)}$. In other words, the encrypted image can be decrypted by iteratively calculating the following formula $n$ times as

$$\boldsymbol{J}(x, y)^{(k)} = A^{(-1)}\ \boldsymbol{J}(x', y')^{(k-1)} (\bmod N) \qquad (3)$$

Arnold transform has a property that the original image will appear when the equation (2) is iteratively calculated $m$ times. The periodicity makes the encryption algorithm directly using Arnold transform unsecure. This is because one can easily obtain the original image by iterative computations once the encryption algorithm is known. The periodicity value $m \leq N$ and some specific values under different image sizes $N$ are listed in Table 1 [7].

| ***N*** | 60 | 100 | 120 | 128 | 256 | 480 | 512 |
|---|---|---|---|---|---|---|---|
| ***m*** | 60 | 150 | 60 | 96 | 192 | 240 | 384 |

Table 1. The Periodicity Values $M$ Under Different Image Sizes $N$

```
$a\,(i, j) \leftarrow 0; i = 1, 2,\ldots.., N; j = 1, 2,\ldots.., N;$
for $i = 2, 3,\ldots.., N-1; j = 2, 3,\ldots.., N-1;$
{
    if $b\,(i, j)$ and $b\,(i + 1, j)$ and [$b\,(i, j + 1)$ or $b\,(i + 1, j + 1)$] and [not [$b\,(i, j - 1)$ or
        $b\,(i + 1, j - 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^0$
    { edge 0 }
    if $b\,(i , j)$ and $b\,(i + 1, j)$ and $b\,(i + 1, j - 1)$ and [not [$b\,(i, j - 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^1$
    { edge 1 }
    if $b\,(i, j)$ and $b\,(i, j - 1)$ and [$b\,(i + 1, \mathrm{j})$ or $b\,(i + 1, j - 1)$] and [not [$b\,(i - 1, j)$ or
        $b\,(i - 1, j - 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^2$
    { edge 2 }
    if $b\,(i, j)$ and $b\,(i , j - 1)$ and $b\,(i - 1, j - 1)$ and [ not [$b\,(i - 1, \mathrm{j})$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^3$
    { edge 3 }
    if $b\,(i, j)$ and $b\,(i - 1, j)$ and [$b\,(i, j - 1)$ or $b\,(i - 1, j - 1)$] and [not [$b\,(\mathrm{i}, j + 1)$ or $b\,(i - 1, j + 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^4$
    { edge 4 }
    if $b\,(i, j)$ and $b\,(i - 1, \mathrm{j})$ and $b\,(i - 1, j + 1)$ and [not [$b\,(i, j + 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^5$
    { edge 5 }
    if $b\,(i, j)$ and $b\,(i, j + 1)$ and [$b\,(i - 1, j)$ or $b\,(i - 1, j + 1)$] and [not [$b\,(i + 1, j)$ or
        $b\,(i + 1, j + 1)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^6$
    { edge 6 }
    if $b\,(i, j)$ and $b\,(i , j + 1)$ and $b\,(i + 1, j + 1)$ and [not [$b\,(i + 1, j)$]]
    then $a\,(i, j) \leftarrow a\,(i, j)$ or $2^7$
    { edge 7 }
}
```

Table 2. Implementation of the Eight Rules for Contour Extraction ($3 \times 3$ Windows)

## 3. Single Step Parallel Contour Extraction (SSPCE) Algorithm

There are two algorithms; 4/8-connectivity scheme s between pixels [11], and 4/8-Directional Freeman chain coding scheme [8] and [9], are used to distinguish all four/eight possible line segments connecting nearest neighbors. The applied algorithm in this work use a $3 \times 3$ pixels window structure to extract the object contours by using the central pixel to find the possible edge direction which connects the central pixel with one of the remaining pixels surrounding it. The algorithm is given exactly the same extracted contours as the OCE algorithms and is much faster (3.8/4.2 times faster) based on which 4/8-Directional Freeman chain coding scheme been used [11]. The edges can be extracted by applying the definition which says that an object contour edge is a straight line connecting two neighboring pixels which have both a common neighboring object pixels which have both a common neighboring object pixel and a common neighboring underground pixel [10]. By this definition, no edges can be extracted from the three following cases:

1- If all nine pixels are object pixels; i.e. the window is inside an object region.

2- If all nine pixels are background pixels; i.e. the window is inside a background region.

3- If the center pixel is an object pixel surrounded by background pixels; i.e. it is most probable that the center pixel in this case is a point noise caused by image digitalization.

The eight rules of edge extraction are applied and are coded using 8-directional chain-code as shown in Table 2.

Many different methods of contour extraction & approximation can be used to gray/color images [12], [13] & [14].

## 4. Image Encryption/Decryption Proposed Scheme

In this section, a different binary image from gray level image is introduced as a "*key image*" with the same size as the original image to be encrypted. We also introduce one image encryption algorithm using this key-image which is referred to the Edge map encrypted algorithm. The analyzed algorithm can fully encrypt 2D such as grayscale images, color images and medical images. The flowchart of the analyzed algorithm is shown in Figure 1.

### 4.1 Bit-planes Generation

Each pixel of a 256 × 256 pixels image in 8bit/pixel (bpp) precision has a gray value between 0 and 255. The entire image can be considered as a two dimensional array of pixel values. We consider the 8bpp data in the form of 8 bit planes, each bit plane associated with a position in the binary representation of the pixels 8 bit data is a set of 8 bit planes. Each bit plane may have a value of 0 or 1 at each pixel, but together all the biplanes makeup a byte with value between 0 to 255. The underlying foundation of the algorithm is to change image pixel values by performing the XOR operation between the key-image and each bit plane of the original image. This is followed by an image scrambling process which changes the locations of image pixels or blocks.

### 4.2 Edge Map Encryption

The edge map is frequently used in image enhancement, compression, segmentation and recognition. The application of edge maps can also be extended to image encryption. In this section, we introduce a new image encryption algorithm using an edge map which is called the Edge map Crypt algorithm. An edge map is considered as the key-image in this algorithm. Such edge map is generated from another different image with the same size as the original image using a specific edge detector with a selected threshold value. The Edge map Crypt algorithm first decomposes the original image into its binary bit planes. Each of them is encrypted by performing an XOR operation with the key image, which is an edge map created from another image. Next, the algorithm inverts the order of all XORed bit planes and combines them together. The resulting image is scrambled by using Arnold transform to generate the final resulting encrypted image. The Edge map Crypt algorithm is illustrated in Figure 2. Similar to the Bit plane encrypted algorithm, a 3D image can be encrypted by applying the Edge map encrypted algorithm to all its 2D components individually. Any new or existing image with the same size of the original image can be used to generate the edge map, the key image. It could be an image in the public online database or a new image generate by the users. The edge map can be obtained by using SSPCE contour extraction algorithm. The users have flexibility to use any existing image scrambling method for the Edge map encrypted algorithm. In this work we used the Arnold transform map. Therefore, the security keys for this algorithm consist of the image or its location which is used to generate the edge map and the security keys of the scrambling algorithm.

### 4.3 Decryption Idea

To reconstruct the original image, the users should be provided the security keys which help them to obtain the correct edge map. The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the inverse Arnold transform.

Next, it decomposes the unscrambled image into its binary bit planes and performs XOR operation between the edge map and each bit plane. The order of all bit planes is restored to the original order. The reconstructed 2D image/component can be obtained by combining all bit planes.

## 5. Statistical Analysis

### 5.1 Histograms

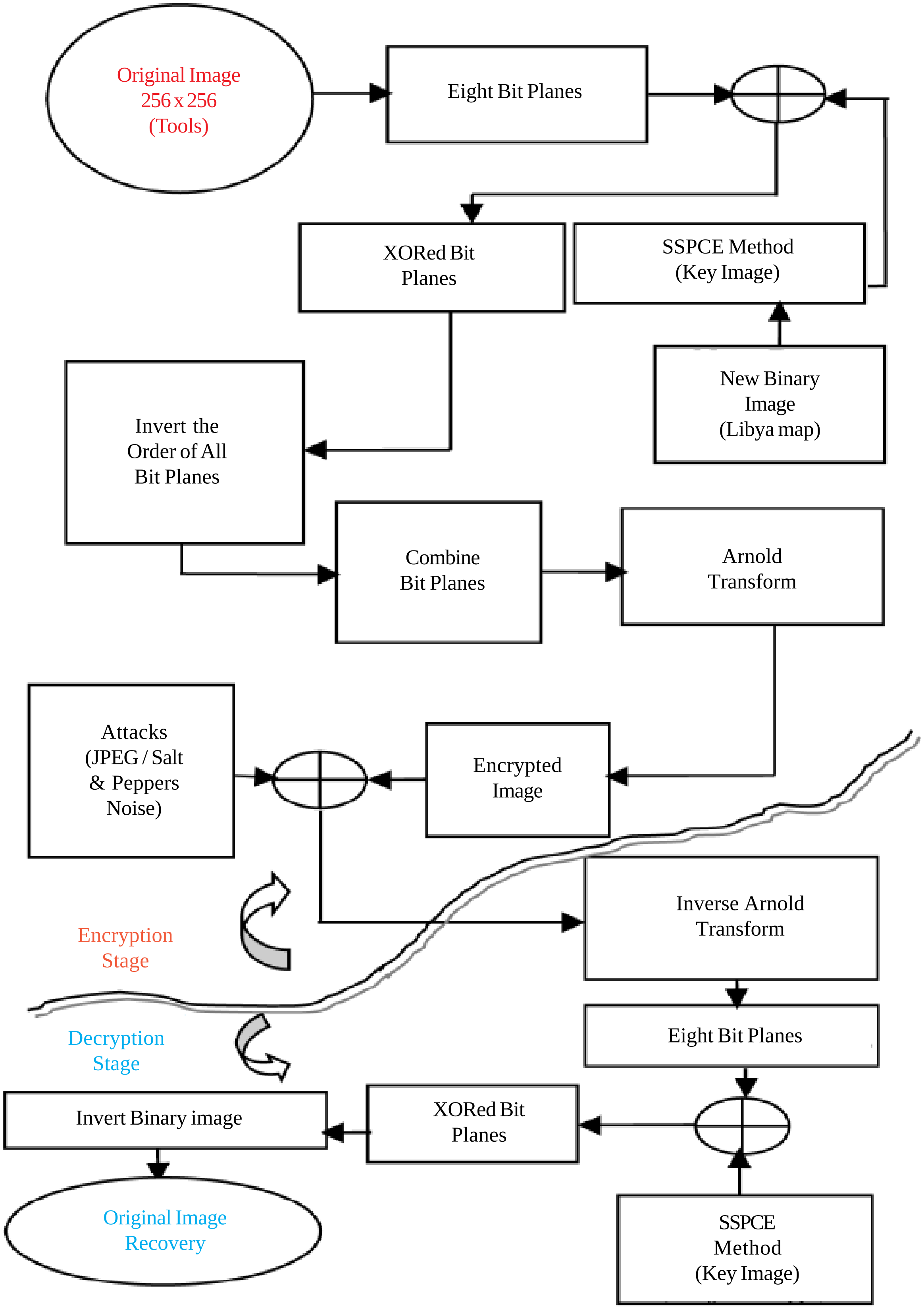


Figure 1. Flowchart of encrypted/decrypted analyzed algorithm

The histogram of an image represents the relative frequency of occurrence of the various gray levels in the image. The histogram of a digital image with gray levels in the range [0, $L - 1$] is a discrete function. The estimate of the probability of occurrence is defines as

$$P\,(r_k) = n_k \,/\, n \tag{4}$$

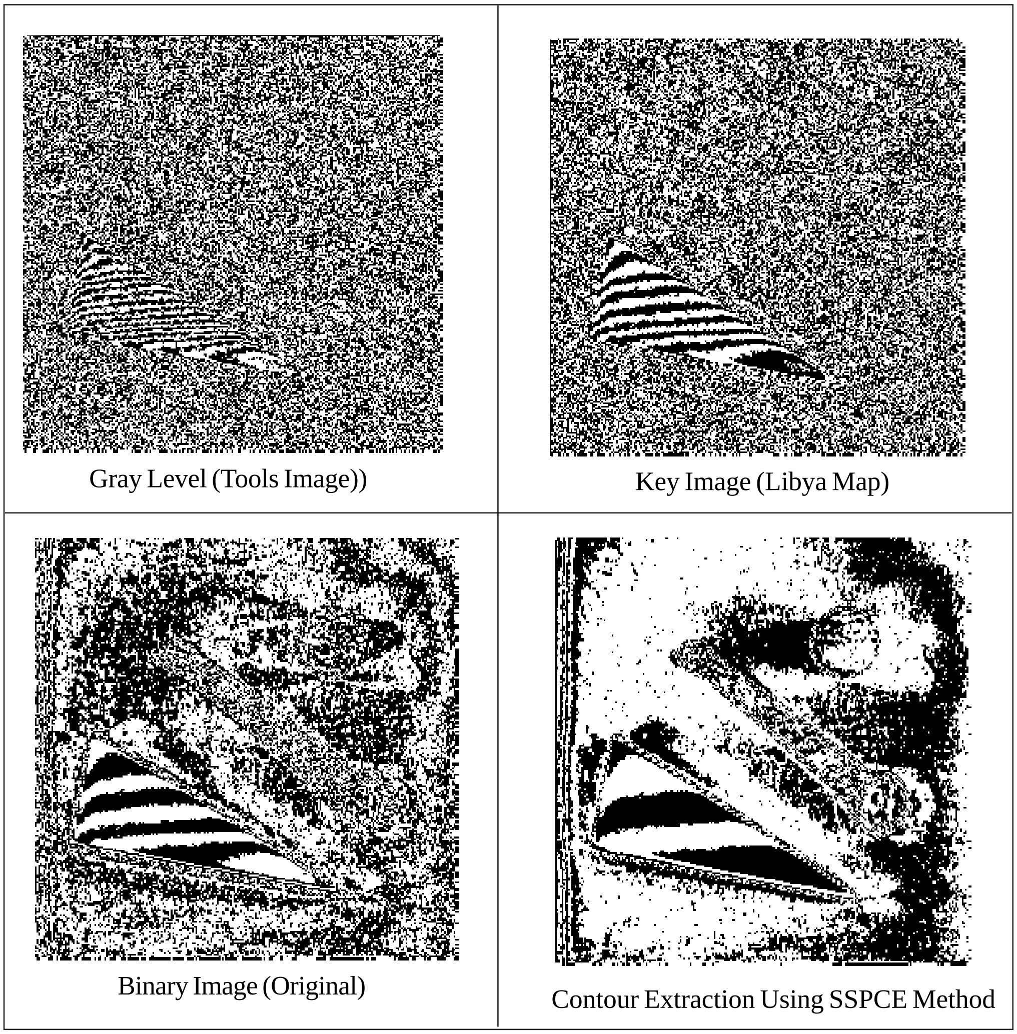
Where, $r_k$ is the $k^{th}$ gray level, $n_k$ is the number of pixels in the image, and $k = 0, 1, 2, 3\ldots\ldots L - 1)$. $P\,(r_k)$ gives an estimate of the probability of occurrence of $r_k$.

For dark images the histogram will be concentrated towards the dark end of the gray scale range. The opposite is true for low contrast images. The histogram of the encrypted image is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration. Moreover, there is no loss of image quality after performing the encryption/decryption steps.

### 5.2 Mean Square Error & Peak Signal-to-Noise Ratio

The mean square error (*MSE*) and peak signal-to-noise ratio (*PSNR*) criterions were used to evaluate the distortion introduced during the image compression and contour extraction procedures. The *MSE* criterion is defined by the following equation

$$MSE\,(I, \tilde{I}) = \frac{1}{(n * m)} \sum_{i=0}^{n} \sum_{j=0}^{m} (I\,(i, j) - \tilde{I}\,(i,\, j)) \tag{5}$$



Gray Level (Tools Image))

Key Image (Libya Map)

Binary Image (Original)

Contour Extraction Using SSPCE Method

Figure 2. Original gray level & key images

where $I$ and $\widetilde{I}$ are the grey-level and reconstructed images respectively.

The *PSNR* is defined by the following formula

$$PSNR\,(I, \widetilde{I}\,) = 10 \log_{10} \frac{(L-1)^2}{MSE\,(I, \widetilde{I}\,)} \tag{6}$$

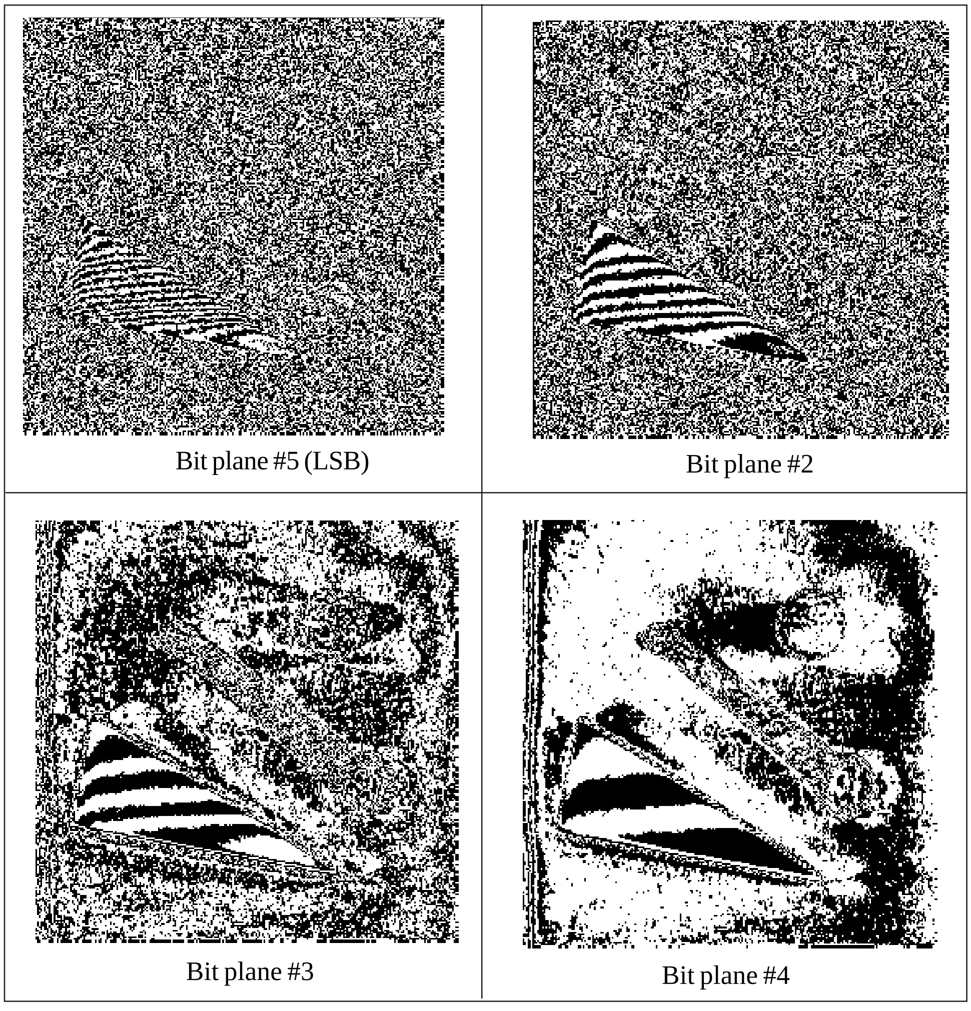
where $L$ is the grey-level number.

### 5.3 Correlation Coefficient

The A single summary number that gives you a good idea about how closely one variable is related to another variable. The correlation coefficient, denoted by $r_{xy}$, is a measure of the strength of the straight-line or linear relationship between two variables. The correlation coefficient takes on values ranging between +1 and –1. The correlation coefficient will vary from –1 to +1. *A* –1 indicates perfect negative correlation, and +1 indicates perfect positive correlation. It’s a measure that determines the degree to which two variable’s movements are associated.

A correlation coefficient is a statistical measure of the degree to which changes to the value of one variable predict change to the value of another. In positively correlated variables, the value increases or decreases in tandem. In negatively correlated variables, the value of one increases as the value of the other decreases. The correlation coefficient between images $X$ and $Y$ can be written as

$$r_{xy} = \frac{\sum_{i=0}^{n} (X_i - \overline{X})\,(Y_i - \overline{Y})}{\sqrt{\sum_{i=0}^{n} (X_i - \overline{X})^2 \sum_{i=0}^{n} (Y_i - \overline{Y})^2}} \tag{7}$$

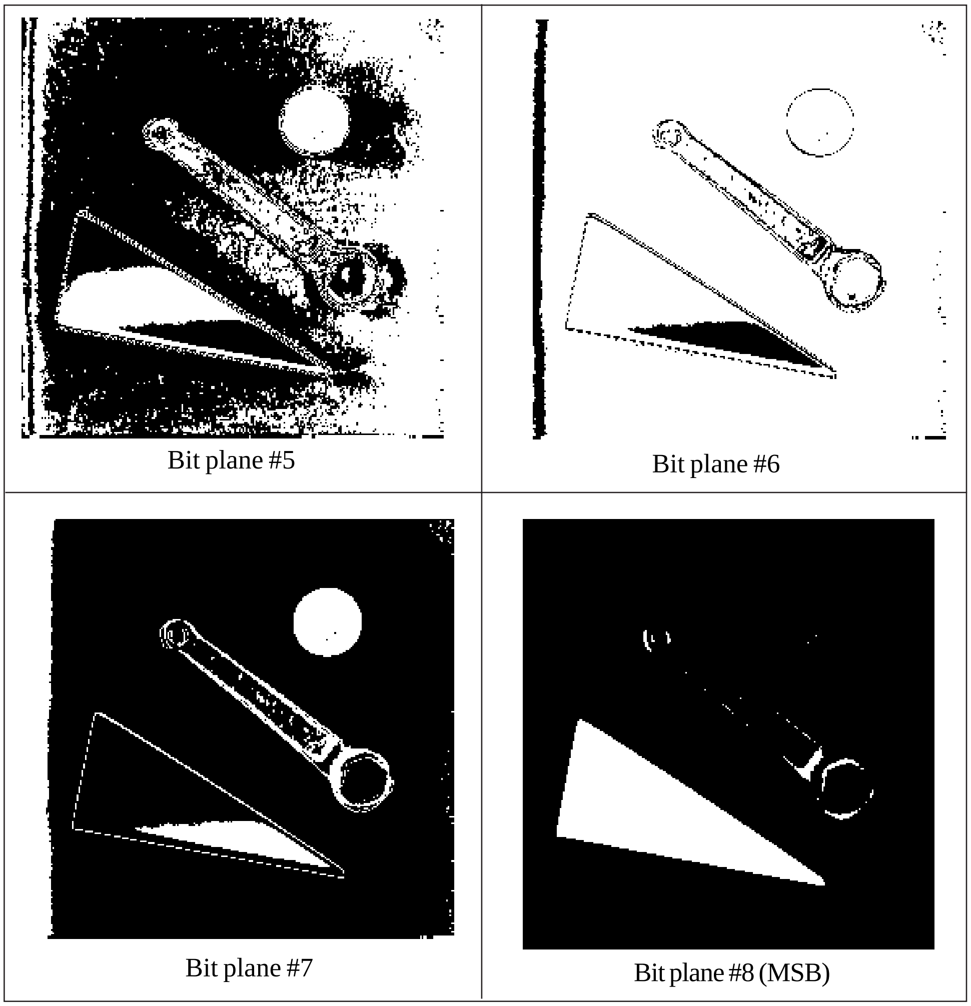


Bit plane #5 (LSB)

Bit plane #2

Bit plane #3

Bit plane #4



Bit plane #5

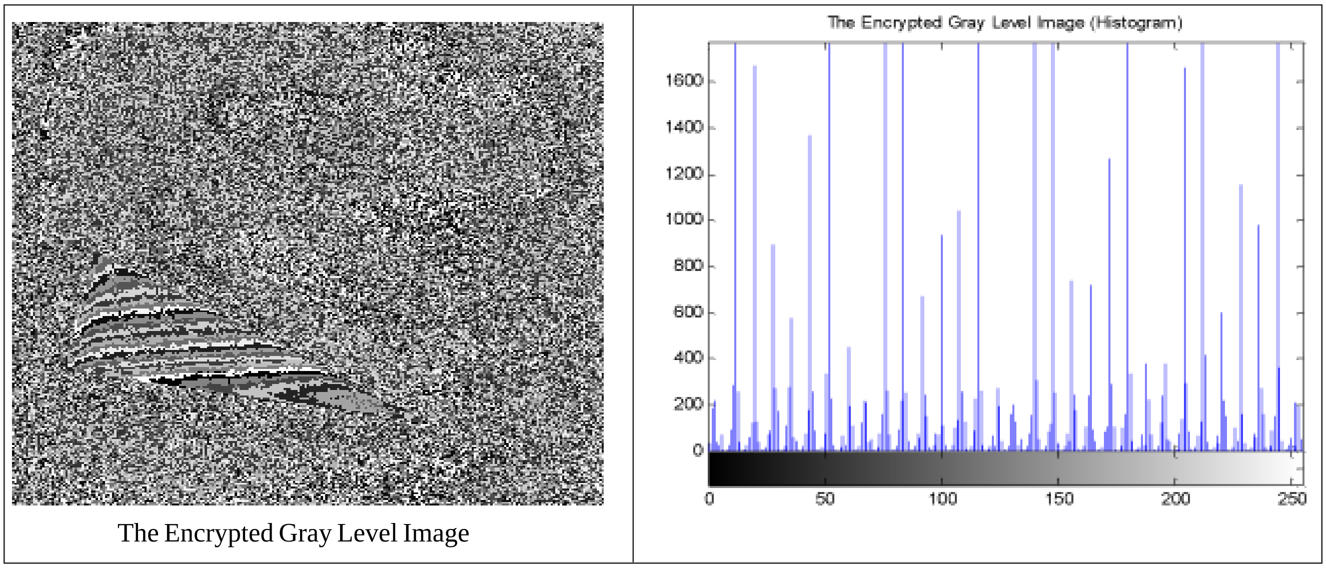
Bit plane #6

Bit plane #7

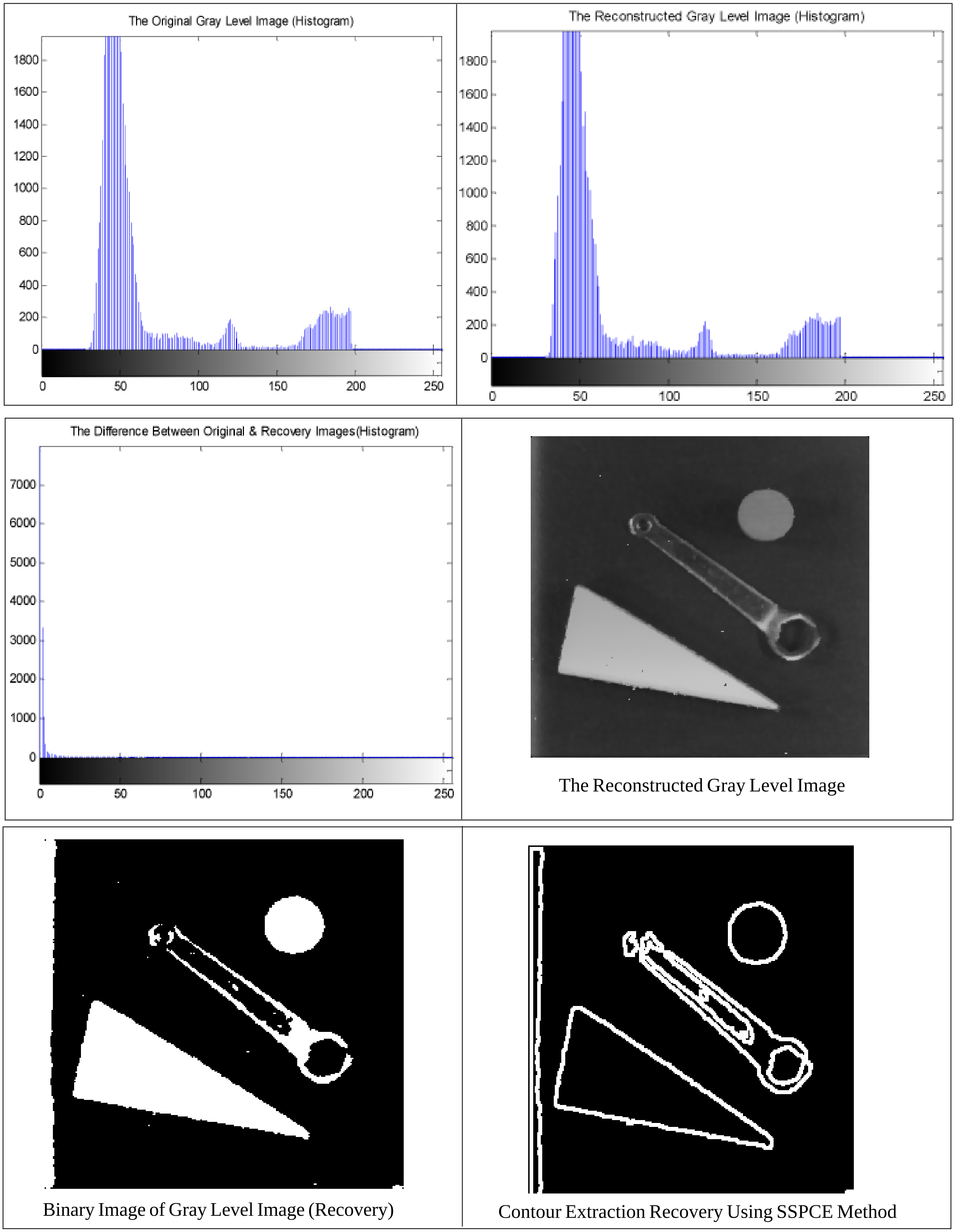
Bit plane #8 (MSB)

Figure 3. Original bitplanes decomposition

where $\bar{X}$ and $\bar{Y}$ are mean of original & reconstructed greylevel images respectively.



The Encrypted Gray Level Image

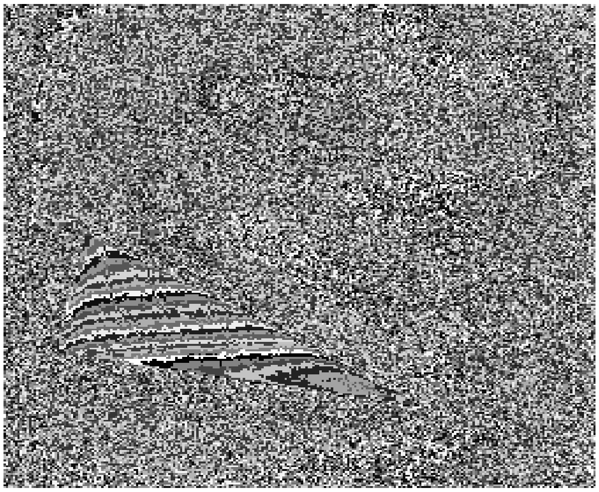


The Reconstructed Gray Level Image

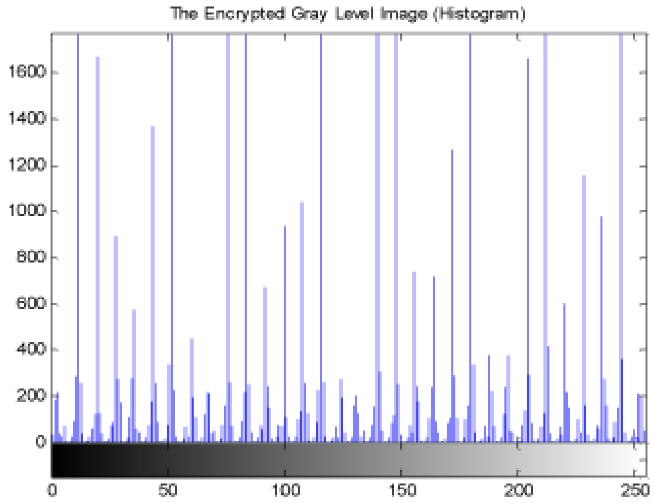
Binary Image of Gray Level Image (Recovery)

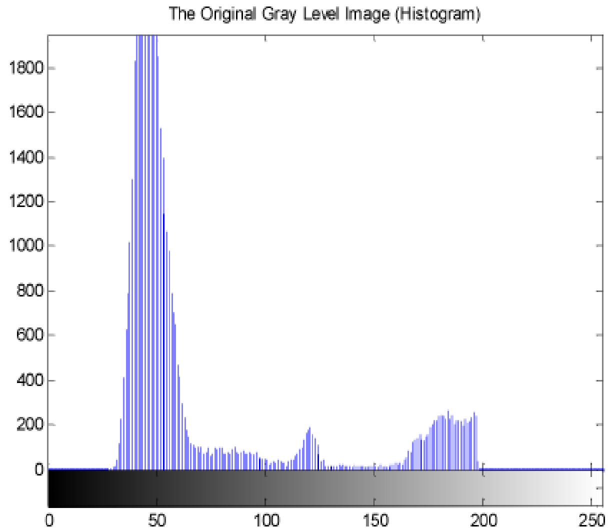
Contour Extraction Recovery Using SSPCE Method

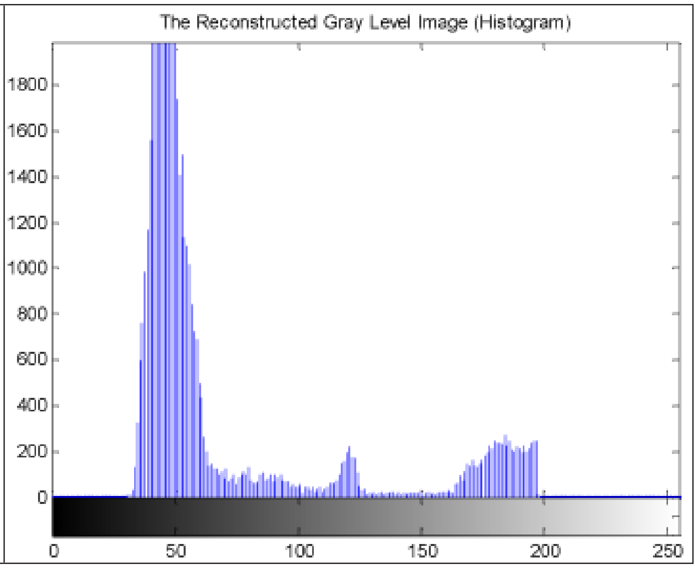
Figure 4. Results using JPEG compression (Corelation Coefficient = 0.9955)

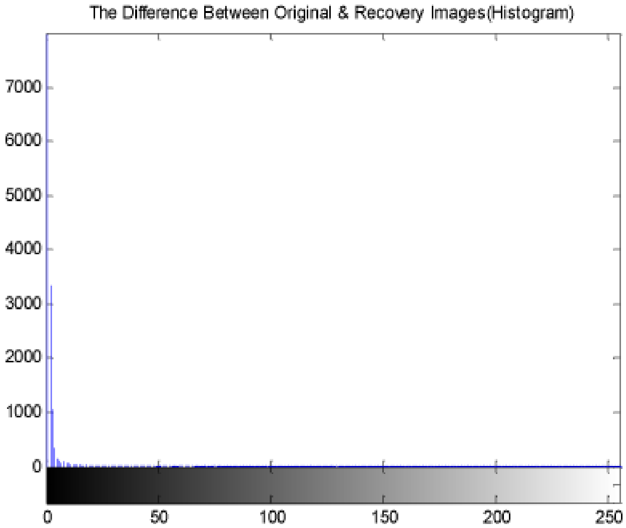


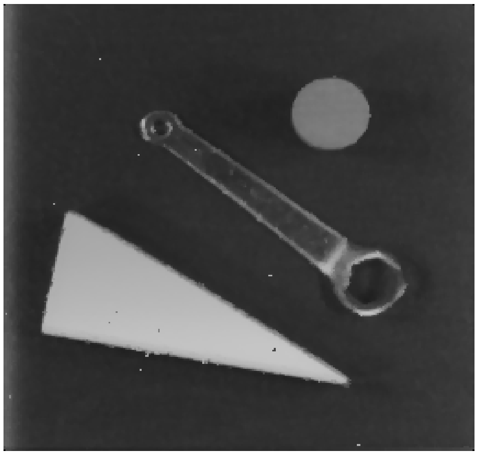
The Encrypted Gray Level Image



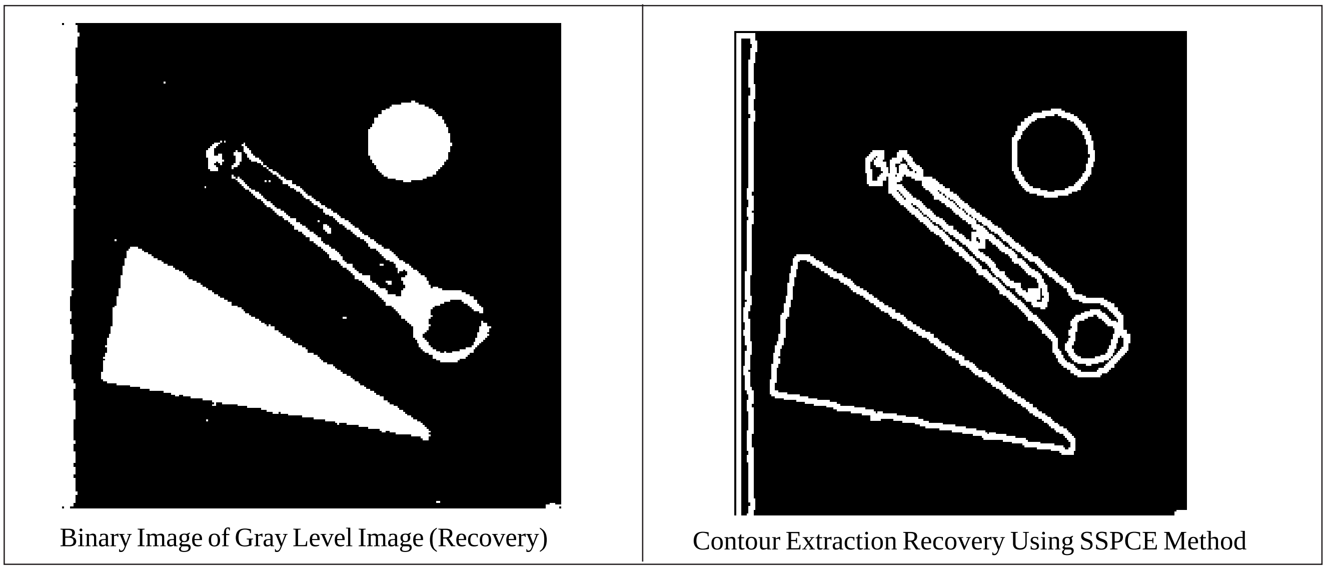








The Reconstructed Gray Level Image



Binary Image of Gray Level Image (Recovery)

Contour Extraction Recovery Using SSPCE Method

Figure 5. Results using Salt & Peppers Noise (Corelation Coefficient = 0.9979)

| Gray Level Image | MSE | PSNR | Correlation Coefficient |
|---|---|---|---|
| Reconstructed | 2.5757 | 44.0219 | 0.9955 |
| JPEG | 49.4791 | 31.1866 | –0.0067 |

Table 3. Original, JPEG & Reconstructed Gray Level Images Comparison Using Jpeg Attackks

| Gray Level Image | MSE | PSNR | Correlation Coefficient |
|---|---|---|---|
| Reconstructed | 2.7047 | 43.8096 | 0.9979 |
| Salt & Peppers | 53.2767 | 30.8654 | –0.0057 |

Table 4. Original, JPEG & Reconstructed Gray Level Images Comparison Using Salt & Peppers Noise Attack

## 6. Experimental Results

The 3D image encryption using the presented algorithm can be accomplished by encrypting all the 2D components one by one. Figures 2 show the gray level (Tools) & binary key (Libya map) images. The binary image of the grey level image Using suitable threshold value & edge map of key image using SSPCE method are also shown in the Figure 2. Figure 3 illustrate he eight bit planes of the gray level (Tools). In Figure 4 & Figure 5, the results (related results are shown in the Table 3 & Table 4 respectively) show that the gray level images are fully encrypted and then completely reconstructed using JPEG compression/ salt & peppers noise attacks respectively. The histograms also verified the distributions of the encryption images are equal in the data level range. The reconstructed images and their histograms in demonstrate the complete reconstruction of the original images. These further prove that the edge map encrypted algorithm is lossless encryption method. In addition to that the recovery binary image of the decrypted gray level image can be obtained easily with high quality at the receiver.

## 7. Conclusions

The In this paper, we have introduced a new concept for image encryption using a binary key. The key-image is an edge map in the edge map encrypted algorithm. Experiments have demonstrated that the proposed algorithm can fully encrypt the 2D images. The original 2D image can also be completely reconstructed without any distortion. Cryptanalysis has shown that the algorithm have extremely large security key space and can with stand most common attacks such as the JPEG compression and salt & pepper. Any new or existing image with the same size as the original image can be used to generate the key-image. The single step parallel contour extraction (SSPCE) method are used to create the edge map as a key-image for the edge map encrypted algorithm. The Arnold transform scrambling method can be applied to the presented algorithm. All these ensure the images can be protected with a higher security level. The presented algorithm is easy to implement in hardware because they operate at the binary levels. They are also suitable for multimedia protection in realtime applications such as wireless networks and mobile phone services. The performed simulation uses Matlab2013a programming.

**References**

[1] Furht, B., Socek, D., Eskicioglu, A. M. (2004). Fundamentals of Multimedia Encryption Techniques, Multimedia Security Handbook, CRC Press, p. 93–131.

[2] Sharma, M., Kowar, M. (2008). Image Encryption Techniques Using Chaotic Schemes: A Review.

[3] Srivastava, A. (2012). A Survey Report On Different Techniques of Image Encryption, *International Journal of Emerging Technology and Advanced Engineering*, 2, p. 163-167.

[4] Nemade, V., Wagh, R. (2012). Review Of Different Image Encryption Techniques, *World Journal of Science and Technology*, 2 (3).

[5] Arnold, I. (1998). Geometrical methods in the theoy of ordinary differential equations, (Springer, 1998).

[6] Yushen, L., Yanling, H., Chenye, W. (2010). A Research on the Robust Digital Watermark of Color Radar Images Proceedings, IEEE International Conference on Information and Automation.

[7] Sun, W. (1999). The periodicity of Arnold transformation, *Journal of North China University of Technology*, 11 (1) 29–32.

[8] Freeman, H. (1961). Techniques for The Digital Computer Analysis of Chain Encoded Arbitrary Plane Curves, *In*: Proc. of the National Electrician Conference, p. 421-432.

[9] Jain, A. K. (1989). Fundamentals of Digital Image Processing, New Jersey: Prentice Hall International.

[10] Nabout, A., Su, B., Nour Eldin, H. (1995). A Novel Closed Contour Extractor, Principle and algorithm, *In*: Proc. Of the International IEEE/ISCAS Conf. on Circuits and Systems, April 29 – May 3, Seattle, USA, 1, p. 445-448.

[11] Besbas, W. (1998). Contour Extraction, Processing and Recognition, Poznan University of Technology, Ph. D. Thesis.

[12] Dziech, A., Ukasha, A., Baran, R. (2006). Fast method for contour approximation and compression, WSEAS Transaction on Communications, p. 49-56.

[13] Ukasha, A. (2010). Arabic Letters Compression using New Algorithm of Trapezoid method, International Conference on Signal Processing, Robotics and Automation (ISPRA'10), Cambridge, United Kingdom, p. 336-341.

[14] Ukasha, A., Hassan, M. (2014). High Quality Extracted Contour from Digital Image Watermarking using DCT & DWT Transforms, International Scientific Academy of Engineering & Technology (ISAET), April, Bangkok, Thailand, p. 5-11.