Lossless Encryption for Color video using a Binary Key-Image

Swati G. Devakate
Student, SVERI'S College of Engineering,
Pandharpur.

S.M. Mukane
SVERI'S College of Engineering,
Pandharpur

ABSTRACT

The science of cryptography has recently attracted significant attention, as more information is stored and transmitted in electronic form. Cryptography is the discipline of using codes to encrypt data into an unreadable format that only the targeted recipient can decrypt and read. Lossless Encryption for Color video using a Binary Key-image. The condition, the key image size is either same or less than the original images. The key image is either a bit plane or an edge map generated from another image. The lossless image encryption algorithms using this key image technique. The key is selected to the grayscale image for new/existing grayscale image and the key is selected to the color image for new/existing color image of video. The code is done in both grayscale and color images using lossless encryption algorithms. The execution of these algorithms is discussed against common attacks such as the plaintext attacks, brute force attack and cipher text attacks. The security analysis and experimental results show that the proposed algorithms can fully encrypt all types of images of video. This makes them suitable for securing video surveillance systems, multimedia applications and real-time applications such as mobile phone services.

Keywords

Lossless video encryption, key-image, plaintext attack, brute force attack, ciphertext attack, bit plane, edge map**.**

1. INTRODUCTION

Cryptography is one of the main pillar of information security. Its usage and usefulness has exploded with the arrival and rise of internet. Cryptography has become essential part of today's information system, and is being exploited in many computing areas such as remote access, online orders and payments, email and messaging security.

Visual surveillance systems and networks make remote video monitoring available for homeland security purpose and also easy to transmit and share videos and image data. With the ubiquitous deployment of visual surveillance systems in many important areas such as airports, commercial centers and also military strategic places, large amounts of videos and images with security information are generated, transmitted and stored.

Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. Several data encryption algorithms like Data Encryption Standard (DES) [1] and Advanced Encryption standard (AES) [2] are proposed for encrypting images. Image encryption can be accomplished by block-based transformation algorithm which is based on the pixel value rotation of image [3]. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed, as well as the possibility of exploiting the correlation between color bands [4]. The image encryption algorithm can also uses DCT to convert target image into frequency domain [5]. And the image encryption for RGB images supported by lifting scheme based lossless compression, in this compress the input color image using a 2-D integer wavelet transform [6].

Applications in the automobile, medical, Construction and the Fashion industry require designs, scanned data, building plans and blue-prints to be safe guarded against espionage. To achieve higher levels of security, solution is to change image pixel values or blocks while scrambling the positions using different techniques.

There are two lossless image encryption algorithms,

i. BitplaneCrypt algorithm.

ii. EdgemapCrypt algorithm.

Using a concept of a binary "key-image", with the same size of the original image to be encrypted. The bit plane crypt algorithm generates the key-image by extracting a binary bit plane from another new or existing image. The other algorithm is an edge map obtained from a new or existing image using a specific edge detector with a specified threshold. The algorithms decompose the original image into its binary into its binary bit planes. The bit planes are encrypted by performing an XOR operation with the key image one by one. And then the order of all bit planes is inverted. And combine all bit planes. The resulting encrypted image can be obtained by applying a scrambling algorithm to the image/Video.

Image security is a major challenge in storage and transmission applications. For example, medical images with a patient's records may be shared among the doctors in different branches of a health service organization over networks for different clinical purposes. These images and videos may contain private information. Providing high security for these images and videos becomes an important issue for individuals, business and governments as well.

In this paper is organized as, Proposed algorithm in section II. Section III Pre-Requisites for Video Encryption, Section IV describes the simulation results. Concluding remarks are made in Section V.

2. IMAGE/VIDEO ENCRYPTION ALGORITHM

The following algorithm is used 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.

2.1 The BitplaneCrypt algorithm for 2D image

The BitplaneCrypt algorithm uses a binary bit plane as the key-image of a video. The algorithm is described in Fig. 1.

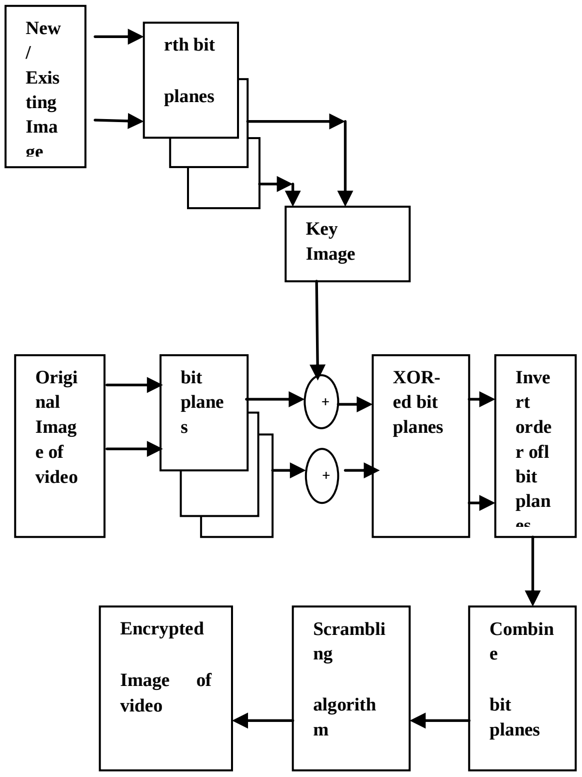

Figure1. BitplaneCrypt Encryption algorithm (For Grayscale Images).

The original image decomposes the binary bit planes. And the new or existing image decomposes bit planes and the key image by exacting the rth bit plane of the selected image of video, where r is the location of bit plane.

The key-image size is same as the original image of the video. Perform the XOR operation between the key image and each bit plane of the original image of video, the XOR-ed bit planes are invert the order of all bit planes and combined. Finally scramble the resulting image using a selected scrambling method to generate the resulting encrypted images for a video. The users have flexibility to choose any new/existing image to generate the key image. This image can be a public image or an image created by the users themselves. The key-image can be selected from one of the bit planes of this image. Therefore, the security keys of the algorithm consist of the image or the location of the image used to generate the key-image.

2.2 The BitplaneCrypt algorithm for 3D image

The 3D image or RGB (Red Green Blue) image of video, assuming i, consider

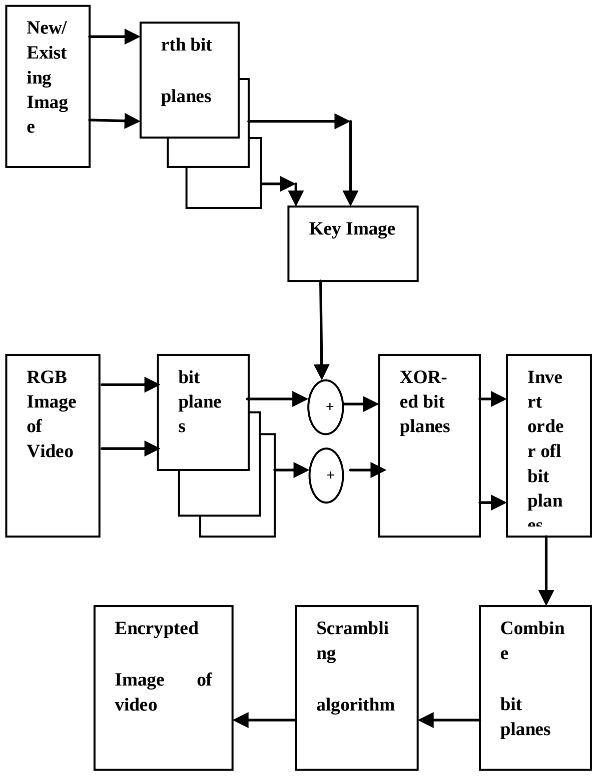

Figure2. BitplaneCrypt Encryption algorithm (For 3D Images).

i= {1 for R,

2 for G,

3 for B.

The algorithm then decomposes the original image i into binary bit planes and performs an XOR operation between each of these bit planes and key-image and the order of bit planes are inverted. The resulting encrypted image can be obtained by applying a scrambling algorithm to the image from a combination of all bit planes.

The BitplaneCrypt Algorithm

Input: The original 3D image (assuming i) to be

Encrypted.

Step 1: Choose a new or existing image with the

same size of the original image.

Step 2: Obtain the key image by extract rth bit plane

of the image in Step 1.

Step 3: Consider *i={1 (R),*

2 (G),

3 (B).

Step 4: Decompose the original image i into binary

Bit planes.

Step 5: Perform the XOR operation between the key-

Image and each bit plane in Step 4.

Step 6: Invert the order of all bit planes.

Step 7: Combine all bit planes together to obtain the

3D image.

Step 8: Scramble the resulting image using a selected

Scrambling method to generate the resulting

Encrypted image.

Output: The encrypted 3D image.

2.3 BitplaneCrypt Decryption algorithm (For 2D Image & 3D *image)*

The decryption process, first apply the unscrambling algorithm to the encrypted image (2D Image or 3D Image) using the selected scrambling algorithm and it decomposes the unscrambled image into binary bit planes and perform the XOR operation between the key image and each bit planes. The users should be provided the security keys which help them to obtain the correct edge map.

The order of all bit planes is restored to the original order and combines all bit planes. The resulting image is the original image of video. The BitplaneCrypt decryption algorithm illustrated in Fig. 3.

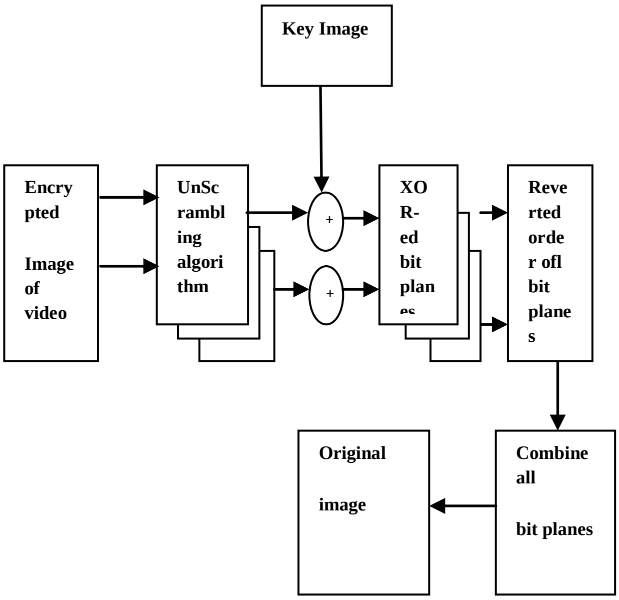

Figure3. BitplaneCrypt Decryption algorithm.

3. PRE-REQUISITES FOR VIDEO ENCRYPTION

Calculate number of frames present in the video and also calculate gray level of each frame. In a graph x-axis shows number of frames and Y-axis shows gray level for each frame.

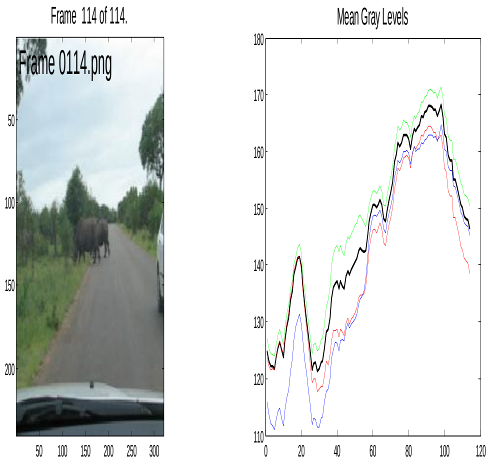

Figure 4. Video clip and calculated gray level as shown in graph

4. EXPERIMENTAL RESULTS

The simulation results are provided to show the performance of the algorithms for grayscale and color image encryption.

4.1 Grayscale or 2D image Encryption for video

The grayscale Images of a video can be successfully encrypted using Bitplanecrypt algorithm.

Figure 5. Shows that an example of grayscale image encryption using the BitplaneCrypt algorithm. The key image in fig. 5(a) is bit plane for grayscale image. As a result, the original image in fig. 5(d) is fully encrypted as shown in Fig. 5(f) and the reconstructed image is same as the original image. This is one advantage of the presented algorithms. The histogram is calculated in Fig. 5(b), and hidden image is generated at threshold 70 in fig. 5(c). The hidden image is inserted in original image as shown in fig. 4(e).

The Gaussian Noise is added to the watermarked image in fig. 4(g), recovered watermark without noise is in fig. 5(h) and with noise in fig. 5(i).

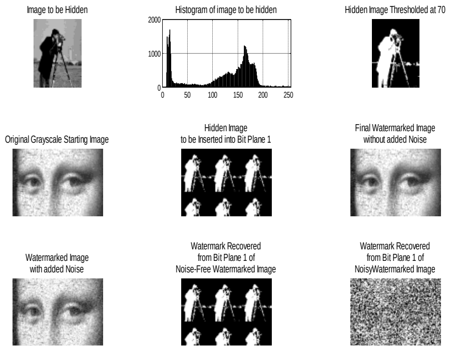
Image to be Hidden
Histogram of image to be hidden
2000
1000
0
0 50 100 150 200 250
Hidden Image Thresholded at 70
Original Grayscale Starting Image
Hidden Image to be Inserted into Bit Plane 1
Final Watermarked Image without added Noise
Watermarked Image with added Noise
Watermark Recovered from Bit Plane 1 of Noise-Free Watermarked Image
Watermark Recovered from Bit Plane 1 of NoisyWatermarked Image

Figure 5. Grayscale image encryption using the BitplaneCrypt algorithm.

(a) The image to be Hidden; (b) A Histogram of hidden image; (c) The Hidden image at Threshold; (d) Original image; (e) Hidden Image to be Inserted; (f) Final Watermarked image without Noise in (d); (g) Noise-free recovered watermark; (h) Noisy Recovered Watermark.

5. CONCLUSION

The Lossless Encryption for Color Images of video using a Binary Key-image is introduced and generate key image as a bit plane in the BitplaneCrypt algorithm.

The grayscale images are fully encrypted from BitplaneCrypt algorithm and completely reconstruct the 2D images and 3D images without any distortion from the original image. The key image size is generated from existing image, which as the same size as original image.

6. REFERENCES

[1] National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[2] National Institute of Standards and Technology, "Advanced Encryption Standards (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[3] Image Encryption by Using Pixel Value Rotation Honnaraju B, Manoj Kumar M,Shiva Sumanth Reddy.

[4] R. Gopinath and M. Sowjanya, M.tech.Student, Sri Indu College of Engineering & Technology, Hyderabad and Associate Professor, Sri Indu College of Engineering & Technology, Hyderabad, "Image Encryption For Color Images Using Bit Plane And Edge Map Cryptography Algorithm", International Journal of Engineering Research & Technology (IJERT). Vol. 1 Issue 8, October – 2012.

[5] Riccardo Lazzeretti, Mauro Barni, "Lossless compression of encrypted grey-level and color images", Department of Information Engineering (University of Siena)

[6] Sara Tedmori and Nijad Al-Najdawi, "Lossless image cryptography algorithm based on DCT", The International Arab Journal of Information Technology.

[7] Simhadri Kollu and P. Soundarya, " Lossless Encryption for Color Images using a Binary Key-image", simhadri kollu international journal of advanced engineering sciences and technologies vol no. 9, issue no. 2, 314 – 321.

[8] Mu Li, Student Member, IEEE, and Vishal Monga, Member, IEEE, "Robust Video Hashing via Multilinear Subspace Projections", IEEE transactions on image processing, vol. 21, no. 10, october 2012.

[9] Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward, Fellow, IEEE, "A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting", IEEE Transactions on information forensics and security, vol. 6, no. 1, march 2011.

[10] Tzuo-Yau Fan Bin-Chang Chieu and Her-Chang Chao, "Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques" , National Taiwan University of Science and Technology Department of Electronic Engineering Taipei, Taiwan.

[11] Shujun Li, Guanrong Chen, Fellow, IEEE, Albert Cheung, Member, IEEE, Bharat Bhargava, Fellow, IEEE and Kwok-Tung Lo, Member, IEEE, "On the Design of Perceptual MPEG-Video Encryption Algorithms", IEEE transactions on circuits and systems for video technology, vol. 17, no. 2, pages 214-223, february 2007.

[12] Tzuo-Yau Fan Bin-Chang Chieu and Her-Chang Chao," Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques" National Taiwan University of Science and Technology Department of Electronic Engineering Taipei, Taiwan, Journal of Electronic Imaging 21(4), 043018 (Oct–Dec 2012)

[13] Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward," A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting", IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.

[14] "The Essential guide to video processing" by AL BOVIK.

[15] Sunil Lee *and* Chang D. Yoo," Robust Video Fingerprinting for Content-Based Video Identification", IEEE transactions on circuits and systems for video technology, vol. 18, no. 7, july 2008.Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender