

BACKWARDS COMPATIBLE, MULTI-LEVEL REGIONS-OF-INTEREST (ROI) IMAGE ENCRYPTION ARCHITECTURE WITH BIOMETRIC AUTHENTICATION

Alexander Wong and William Bishop

Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada

Keywords: Multi-level image encryption, ROI, backwards compatibility, biometrics.

Abstract: Digital image archival and distribution systems are an indispensable part of the modern digital age. Organizations perceive a need for increased information security. However, conventional image encryption methods are not versatile enough to meet more advanced image security demands. We propose a universal multi-level ROI image encryption architecture that is based on biometric data. The proposed architecture ensures that different users can only view certain parts of an image based on their level of authority. Biometric authentication is used to ensure that only an authorized individual can view the encrypted image content. The architecture is designed such that it can be applied to any existing raster image format while maintaining full backwards compatibility so that images can be viewed using popular image viewers. Experimental results demonstrate the effectiveness of this architecture in providing conditional content access.

1 INTRODUCTION

Digital image management systems have become an integral part of many organizations, ranging from hospitals to military institutions. The popularity of storing scans of confidential documents as images has led to the need for increased support for image encryption. Examples of scanned document images include military maps, legal agreements, and medical documents. Such confidential images are often encoded as binary data and protected using conventional cryptographic techniques such as block ciphering systems.

A number of image encryption algorithms using conventional techniques have been proposed and investigated (Dang and Chau, 2000; Hou and Wang, 2003; Ziedan et al., 2003). Image-specific cryptographic techniques also exist (Seo et al., 2003; Chen et al., 2005; Salleh et al., 2003; Zhang et al., 2003). Such techniques utilize the characteristics of images to yield better overall computational performance, but have been shown to be less secure than conventional techniques (Li et al., 2004a; Li and Zheng, 2002a; Li et al., 2004b; Li and Zheng, 2002b). While such cryptographic techniques are effective for providing file-level security for documents, the techniques diminish

the legibility of the images and render them useless in content-based document searches. More importantly, existing cryptographic techniques are not designed to provide image encryption capabilities for specific regions of interest (ROI). This feature is very important for concealing only the information that needs to be protected while making the rest of the image available for general viewing. Traditional image encryption algorithms also fail to provide different levels of access to a document image. This feature is important in situations where different users are authorized to view some but not all of a document image. Therefore, traditional image encryption algorithms are not versatile enough to fulfill many important advanced encryption requirements.

Recently, an extension to JPEG 2000 known as JPSEC (Dufaux et al., 2004) was proposed as a framework for securing image content. One of the tools provided by this framework is the ability to support conditional access to an image. This feature allows access to regions of an image to be restricted. One approach to accomplishing this using JPSEC is presented in (Dufaux et al., 2004; Dufaux and Ebrahimi, 2004) where the information within specified regions is scrambled with pseudorandom noise. The seed val-

ues used to generate the pseudorandom noise are then encrypted and placed inside the JPSEC codestream. The receiver can then use the encryption key to retrieve the seeds for the purpose of descrambling the regions. Furthermore, the use of multiple encryption keys enables the ability to provide multiple levels of access to the image. JPSEC effectively provides a solution for multi-level ROI image encryption.

There are a number of important issues that are not currently addressed by JPSEC. First, the conditional access approach used by JPSEC is integrated into the JPEG 2000 framework. This approach cannot be easily used for many popular formats including TIFF, BMP, GIF, PNG, and JPEG. This limitation is particularly important since JPEG 2000 is not yet widely supported by image editing and web browsing applications. The lack of a backwards compatibility for JPSEC is a limiting factor for its usefulness. Another important issue is that JPSEC does not provide an explicit means to authenticate the user. This is problematic for securing highly confidential data. If an attacker is able to obtain the encryption keys, the attacker gains full access to the secured image content. Obtaining encryption keys is often made easier by the fact that strong encryption keys are very difficult to remember and are often secured by weak passwords that are easy to crack. Therefore, a secure method is desired to ensure that the user accessing the content is actually an authorized individual.

This paper introduces a backwards compatible, multi-level ROI image encryption architecture using biometric authentication. The proposed architecture addresses the issues of backwards compatibility and user authentication. These issues are not currently addressed by JPSEC. In this paper, the theories underlying the proposed architecture are presented in Section 2 along with a discussion of the issues associated with backwards compatibility. An outline of the proposed architecture is also provided in Section 2. Experimental results demonstrating the effectiveness of the proposed architecture are presented in Section 3. Finally, conclusions are drawn and future work is discussed in Section 4.

2 THEORY

Prior to outlining the proposed image encryption architecture, it is important to introduce some of the theory behind the key concepts of the architecture. First, the basic concept of multi-level ROI encryption is presented along with a simple method of implementing such a system. This serves as a building block for the proposed architecture. The issues dealing with

backwards compatibility are described in detail and practical solutions are provided to clarify how such a system can be integrated into existing widely used image formats while maintaining format compliance. Finally, the concept of biometric authentication is explained in detail along with a method to integrate such a technique into the system to ensure only authorized individuals are given access to the image content.

2.1 Multi-level ROI Encryption

The goal of multi-level ROI encryption is to encrypt an uncompressed raster image such that an image viewer can view specified regions within the image based on authentication. Multi-level ROI encryption allows a single image to be used by several users for different purposes. Upon creation, the levels of authentication are specified and regions of interest are assigned to each of the levels of authentication. Consider the following example. Alice would like to post a legal document in the form of a scanned document image for Bob, Carol, and Donna to validate. Alice wants Bob to check the legal validity of the terms in the contract but does not want Bob to know the names of the parties involved or the signatures of the parties. Alice wants to give Carol a higher level of access than Bob to view the terms of the contract as well as record the names of the parties involved but does not want Carol to see the signatures of the parties for privacy reasons. Finally, Donna is Alice's manager and so Alice would like to give Donna full access to the scanned document image. Multi-level ROI encryption allows for this type of flexibility by encrypting the image such that the specified access rights may be ensured. As such, Alice is able to e-mail the same scanned document image to all three individuals without the need to create three versions of the document.

Consider another important example. A company that provides high-resolution satellite images would like to post the maps on a public website. It is desirable for the general public to be able to view most of the map with the exception of certain restricted government sites. However, for military use the restricted government sites could be accessible to army officers with the appropriate security clearance level. Multi-level ROI image encryption provides support for this functionality.

For the purpose of the proposed algorithm for multi-level ROI image encryption, the sender inputs an image into the image encryption system along with information about the ROI within the image that needs to be encrypted and the level of authority required for each ROI. Typically, the user performs the ROI selection process manually. However, in the

case of standardized document images, systems have been introduced that perform automatic ROI selection (Wong and Bishop, 2006). Such systems have been shown to be effective at reducing human interaction during the encryption process. Automatic ROI selection algorithms simplify the task of encrypting a standard set of document images.

Using the specified ROI information, ROI that lie within the same level of authority i are encrypted with a cipher key CK_i using a secure conventional stream cipher such as RC4, SEAL (Rogaway and Copper-smith, 1998), SCREAM (Halevi et al., 2002) or a block cipher such as DES and AES on a bit-stream level. Therefore, a different cipher key is needed for each available level of authority. This encryption scheme allows for different regions within an image to be encrypted differently depending on the level of authority required to view the region. An example of how the encryption process works is shown in Figure 1.

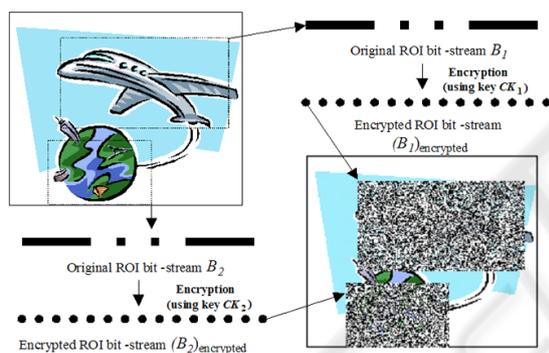


Figure 1: ROI Encryption Process.

If a strong encryption scheme is used with strong cipher keys, the resulting image content in the ROI should resemble random noise. A secure conventional cipher was used as opposed to the pseudorandom noise for a number of reasons. First, while the pseudorandom noise approach used by JPSEC (Dufaux et al., 2004) reduces the complexity of the protection process, it is not a secure method for protecting highly confidential data within an image. This is particularly important for institutions such as government agencies, where confidentiality is a high priority. Therefore, the improved level of security gained from using a conventional cipher outweighs the efficiency gained from using the simple pseudorandom noise approach.

To improve the level of security achieved by this method, a unique identifier (UID) is combined with each encryption key to form a final encryption key

used for each level of authority. What this accomplishes is to ensure that, in the case where stream ciphers are used, different images are encrypted with different key-streams even if they share a common encryption key. Once the ROI of the image have been encrypted, the ROI and level of authority information are stored in the image. Finally the image can be sent to its recipients who can then use the set of encryption keys that they possess based on their level of authority to access encrypted versions of the image.

2.2 Backwards Compatibility

The ultimate goal of this paper is to devise an architecture that allows multi-level ROI image encryption to be used with any widely adopted, raster-based image format. A number of issues need to be addressed for the multi-level ROI image encryption algorithm described in Section 2.1 to be integrated into existing widely used formats such as BMP, TIFF, PNG, JPEG, and GIF while maintaining backwards compatibility. The first issue deals with public content. One motivation for a backwards compatible, multi-level ROI architecture is that there are situations where it is desirable for the general public to be able to view an encrypted image using any standard image viewer or web browsing application, while only individuals with special image decryption software and the appropriate keys can view the encrypted regions of the image that they are authorized to view.

One possible approach to addressing this issue is through the use of a mixed raster content (MRC) model. Using this approach, an image is segmented into multiple layers: a public layer and an encrypted layer for each level of authority. Only those with the appropriate keys can retrieve image content from the encrypted layers. An advantage to this approach is that ROI and level of authority information does not need to be explicitly stored as it is implicitly defined by the layering of the image. However, the main disadvantage to this approach is that most widely used image formats, besides TIFF, do not provide support for layers. Furthermore, segmenting and storing the image as individual layers adds complexity to the problem. Therefore, to allow the architecture to be used by the widest range of popular image formats, a simple approach of storing public and encrypted image content in a single layer is used.

Another issue that needs to be addressed is the storage of additional encryption-related information such as ROI and level of authority information as well as the UID. This can be easily accomplished in formats such as TIFF and JPEG due to the fact that both formats support the storage of custom meta-

data within the image file. Therefore, the encryption-related information can be arranged into a data frame and stored directly in the meta-data area of the image. However, many widely used image formats do not provide a standard for embedding custom meta-data. These include BMP, GIF, and PNG. Therefore, an alternative approach must be devised to store the encryption-related information without affecting format compliance for the algorithm to support such image formats. To remedy this problem, encryption-related information is encoded and then hidden within the image content data itself using digital image watermarking techniques.

The actual encoding scheme for the encryption-related information depends on a number of factors, such as the acceptable shapes of the ROI and the number of levels of authority supported. A sample frame for a 1024×1024 image with 2 regions of interests (A and B) and 2 levels of authority (0 and 1) is shown in Figure 2. One side benefit of storing the encoded encryption-related information directly into the image using watermarking techniques is that no additional storage space is required to hold the information. The watermarking technique is performed after image compression if a lossy image compression scheme is used in the image format. This ensures that the encoded encryption-related information is not lost due to lossy image compression.

$ROI_{count} = 2$ (8 bits)	$A_{level} = 0$ (1 bit)	$A_1 = (3, 3)$ (20 bits)	$A_2 = (40, 40)$ (20 bits)	$B_{level} = 1$ (1 bit)	$B_1 = (50, 60)$ (10 bits)	$B_2 = (100, 200)$ (20 bits)
-------------------------------	----------------------------	-----------------------------	-------------------------------	----------------------------	-------------------------------	---------------------------------

Figure 2: Sample ROI Information Frame.

2.3 Biometric Authentication

A major issue that needs to be addressed is the need for user authentication. This issue is not addressed in JPSEC and related works on image encryption. However, it is very important to ensure that the person viewing the secure content is in fact the person who is authorized to view the information. A traditional method for authenticating a user is through the use of passwords. To access the desired content, the user sends a password to an authentication server. If the password used is correct, the server sends a strong encryption key back to the user which can then be used to decrypt the data. However, this is not very secure since passwords are often short and chosen such that they are easy to remember. An attacker can easily determine passwords using a combination of brute force methods, guesses, or phishing attacks that entice users to reveal passwords. A more effective so-

lution to providing user authentication is through the use of biometric authentication. In biometric authentication, biological characteristics that are unique to the user are used for authentication. These biological characteristics include fingerprints, iris patterns, and speech. Unlike methods using passwords, biometric information is a unique characteristic of an individual and therefore less susceptible to physical theft if the biometric system is properly implemented. There are numerous different biometric recognition methods available depending on the type of biometric data is used. A survey on biometric techniques can be found in (Delac and Grgic, 2004). For the purpose of this research, the focus is on presenting a method for integrating biometric user authentication into the proposed multi-level ROI image encryption architecture.

The basic concept of the proposed biometric approach is similar to that described for password-based authentication. However, rather than sending a password, biometric data pertaining to the user is used to construct a unique biometric key and the biometric key is sent instead. Furthermore, two individuals with the same level of authority must be able to view the same content. Therefore, a way to allow more than one person to the same content is needed.

Recall the example involving Alice, Bob, Carol, and Donna from Section 2.1. This example can be extended to integrate biometric authentication. To do so, we introduce an authentication server (denoted as AS) that also acts as a key management server. As such, the AS possesses a database of biometric templates that include those of the participating parties. When Alice wishes to protect the legal document, she makes a request to the AS for a set of encryption keys (one for each level of authority) and a UID. Alice also sends the AS information regarding the level of authority each of the participating parties have for the image. The AS sends Alice the requested information through a secure channel and stores a record of the UID, the set of generated encryption keys, the level of authority each key is associated with, and the level of authority of each individual. Alice then encrypts the image using the proposed multi-level ROI encryption techniques. The encrypted image is sent to Bob, Carol, and Donna. When Bob views the image, he sends his username, the biometric key constructed using his biometric information, and the UID of the image to the AS through a secure channel. The AS then takes the biometric key and matches it with the biometric template associated with Bob. If the biometric key matches that of the biometric template, the AS retrieves the set of encryption keys associated with the level of authority assigned to Bob by Alice and sends them to Bob. Bob can then use the set of encryption

keys to decrypt the portions of the image that he is authorized to view. When Donna wishes to view the content she is authorized to see, she undergoes the same process that Bob goes through. However, since Donna is at the highest level of authority, she receives the entire set of encryption keys for all levels of authority. This approach allows the encryption keys to be bound to the level of authority and not the individuals. Furthermore this approach ensures that the individuals accessing the information are verified using biometric user authentication. The above example (showing only Alice, Bob, and Carol) is illustrated in Figure 3.

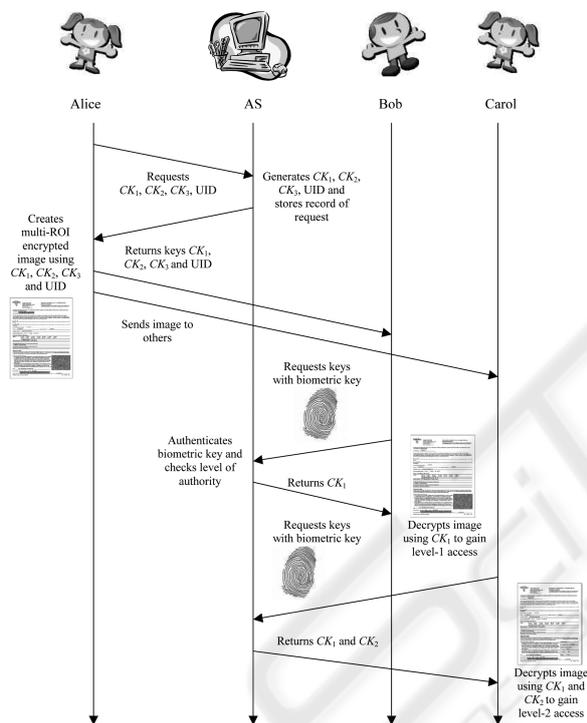


Figure 3: Example image encryption and authentication flow.

3 EXPERIMENTAL RESULTS

For testing purposes, the proposed architecture was implemented as a document management system using the RC4 stream cipher with 128-bit keys and the TIFF format with the lossless PackBits compression scheme. Since the TIFF format was used, the encryption-related information was stored as metadata. The biometric authentication system used for the test system was a simple fingerprint-matching system using normalized correlation. Since any cipher and biometric matching algorithm can be used

in the proposed framework, RC4 and the fingerprint-matching algorithm were chosen for testing purposes due to their simplicity. For scenarios that require a higher level of security, a block cipher such as AES and more advanced biometric authentication techniques can be used. This test system was designed primarily to demonstrate the effectiveness of the proposed image encryption architecture. The test set consists of different document images from the University of Waterloo Registrar’s Office, with multiple ROIs selected for each document image and encrypted at three levels of authority. Four sample encrypted document images are illustrated in Figure 4. These images were obtained using the proposed architecture. It can be seen that the proposed system is effective at maintaining image legibility while providing conditional content access at multiple levels.

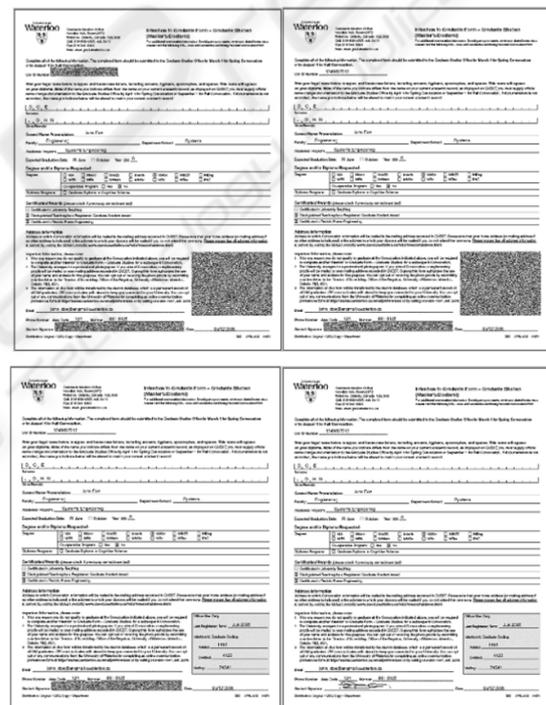


Figure 4: Sample Encrypted Document Images from a 3-level ROI encryption scheme; Top-left: Image encrypted for public viewing; Top-right: Image viewed with level-1 access; Bottom-left: Image viewed with level-2 access; Bottom-right: Image viewed with level-3 access.

4 CONCLUSION

This paper proposes a novel architecture for multi-level ROI image encryption using biometric authentication. The proposed algorithm is highly efficient and

flexible, and can be used with existing widely used image formats. Furthermore, the use of biometric authentication ensures that only authorized individuals have access to secure image data. It is our belief that this method can be successfully implemented in digital image archival and distribution infrastructures to provide flexible image information security. Future work includes the application of the proposed algorithm for multi-level ROI video encryption.

ACKNOWLEDGEMENTS

This research has been sponsored in part by Epson Canada and the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

- Chen, R., Lai, J., and Lu, W. (2005). Image encryption using progressive cellular automata substitution and SCAN. In *Proceedings of the International Symposium on Circuits and Systems*, volume 2, pages 1690–1693.
- Dang, P. and Chau, P. (2000). Image encryption for secure internet multimedia applications. *IEEE Transactions on Consumer Electronics*, 46(3):295–403.
- Delac, K. and Grgic, M. (2004). A survey of biometric recognition methods. In *Proceedings of the 46th International Symposium on Electronics in Marine*, pages 184–193.
- Dufaux, F. and Ebrahimi, T. (2004). Video surveillance using JPEG 2000. In *Proceedings of SPIE: Applications of Digital Image Processing XXVII*, volume 5558, pages 268–275.
- Dufaux, F., Wee, S., Apostolopoulos, J., and Ebrahimi, T. (2004). JPSEC for secure imaging in JPEG 2000. In *Proceedings of SPIE: Applications of Digital Image Processing XXVII*, volume 5558, pages 319–330.
- Halevi, S., Coppersmith, D., and Jutla, C. (2002). Scream: a software-efficient stream cipher. Technical Report 2002/019, Cryptology ePrint Archive. <http://eprint.iacr.org/2002/019>.
- Hou, Q. and Wang, Y. (2003). Security traffic transmission based on EZW and AES. In *Proceedings of IEEE Intelligent Transportation Systems*, volume 1, pages 86–89.
- Li, C., Li, S., Zhang, D., and Chen, G. (2004a). Cryptanalysis of a chaotic neural network based multimedia encryption scheme. In *Proceedings of Advances in Multimedia Information Processing (PCM 2004)*, volume 3, pages 418–425.
- Li, S., Li, C., Chen, G., and Mou, X. (2004b). Cryptanalysis of the RCES/RSES image encryption scheme. Technical Report 2004/376, Cryptology ePrint Archive. <http://eprint.iacr.org/2004/376>.
- Li, S. and Zheng, X. (2002a). Cryptanalysis of a chaotic image encryption method. In *Proceedings of the International Symposium on Circuits and Systems*, pages 708–711.
- Li, S. and Zheng, X. (2002b). On the security of an image encryption method. In *Proceedings of the International Conference on Image Processing*, pages 925–928.
- Rogaway, P. and Coppersmith, D. (1998). A software optimized encryption algorithm. *Journal of Cryptology*, 11(4):273–287.
- Salleh, M., Ibrahim, S., and Isnin, I. (2003). Enhanced chaotic image encryption algorithm based on Baker's map. In *Proceedings of the International Symposium on Circuits and Systems*, volume 2, pages 508–511.
- Seo, Y., Kim, D., Yoo, J., Suijit, D., and Agrawal, A. (2003). Wavelet domain image encryption by subband selection and data bit selection. In *Proceedings of the World Wide Congress (3G Wireless)*.
- Wong, A. and Bishop, W. (2006). Expert knowledge based automatic regions-of-interest (ROI) selection in scanned documents for digital image encryption. In *Proceedings of the Third Canadian Conference on Computer and Robot Vision*, page 51.
- Zhang, H., Feng, W., Hui, L., Hai, L., and Chou, L. (2003). A new image encryption algorithm based on chaos system. In *Proceedings of Robotics, Intelligent Systems and Signal Processing*, volume C16, pages 1–8.
- Ziedan, I., Fouad, M., and Salem, D. (2003). Application of data encryption standard to bitmap and JPEG images. In *Proceedings of the Twentieth National Radio Science Conference*, volume C16, pages 1–8.