Low Color-Depth Image Encryption Scheme for use in COTS Smartphones

NIKOLAOS DOUKAS
Department of Mathematics and Engineering Science, Informatics and Computer Science Lab
Univ. Military Education - Hellenic Army Academy
Vari - 16673,
GREECE
nikolaos@doukas.net.gr

Abstract: - Cyber security and privacy are sources of increasing importance for the successful deployment of information and communication technology. This paper investigates aspects concerning privacy during the communication of low color depth images in encrypted form via low bit-rate, error prone channels. Existing approaches for region of interest determination in images, image encryption and image compression within this context are presented. The problem is established and conflicts between the aims of data compression and data encryption are out-lined and theoretically founded. An innovative approach is hence presented that automatically selects regions of interest in low color depth images, while achieving an acceptable level of security without increasing the data volume of the resulting image. The technique is suitable for cases where the data being transmitted has a limited lifecycle period and the compressed and encrypted image data are likely to be corrupted, such as the transmission via channels that are not guaranteed error – free. An error correction add-on to the algorithm permits an increase on the average decrypted image quality. Initial crypt-analytic resilience results for the proposed scheme are given. The proposed scheme is intended as a means of facilitating the deployment of COTS technology in tactical situations, by increasing the level of security of the underlying infrastructure.

Key-Words: - image encryption; encoding; low resolution; error resilience; COTS

1 Introduction

Information system security has grown over the years from a problem that concerned only military users of Information and Communication Technologies, to the primary concern of civilian and military authorities as well as commercial organizations at all levels of their respective hierarchies. In military and public applications, the introduction of command and control systems has given a new perspective in the efficiency of administration of the forces, but the fact that information systems and transmission networks extend to the last soldier in the field, has greatly increased the importance of managing the risk of some of the content traveling towards the command centers falling on hostile hands. Similar reasoning applies to government organizations that exploit distributed information systems in order to optimize the effectiveness of their administration. Commercial institutions are similarly organized in a distributed manner via exploitation of information systems so as to optimize their efficiency, exploit local manufacturing opportunities, reduce costs of traveling and better market their products and services in local markets by satisfying local particularities.

Communication of image data is of paramount importance both to military applications (e.g. command and control systems) as well as applications like health services (telemedicine, medical records etc). The image signal has its own particular characteristics. Images are in general large in size but may contain a significant amount of redundant information, even after a compression such that offered by standards like jpeg or tiff. Depending on the type of application, the encryption requirements will vary: military applications require that the image becomes totally unrecognizable while the requirements of a subscription television channel might be satisfied with significant degradation of the image quality [1]. The redundant information, when encrypted for security purposes, will give rise to even larger quantities of encrypted data that may not have a reason for existing [1]. It is sometimes feasible to accept the existence of such redundant data in images that are stored and processes off –

line or in systems whit excessive computational and storage capabilities. In certain applications however, where processing power is severely limited and storage and transmission bandwidth scarce, such waste is prohibiting for the use of security algorithms. Such applications include portable devices carried by personnel in the field, facsimile data, remote imaging devices etc. Security analysis of such systems is still an open issue [2], since cryptanalytic research focuses mainly on the needs of encryption of abstract data, without taking into consideration the needs of multimedia processing [2]. A fundamental problem in multimedia encryption is splitting the data stream into meaningful part, in a way such that no particular part alone is sufficient to attackers [3]. Another important open issue is concerned with removing the excessive redundancy contained in the image data, so as not to strain the system bandwidth [4]. An interesting approach is presented to this respect in [4] that additionally aims to exploit the data compression process as an additional encryption step. Further approaches for reducing the data volume by selecting the regions of interest are reported in [5]. A method for reducing the correlation present in images, due to the large areas of the background, is given in [6] and uses a pixel permutation block before the encryption. An attempt to simplify scanned document encryption, so that it may be implemented on an autonomous, FPGA based device was presented in [7]. A hierarchical encryption scheme that offers a beneficial compromise between the speed of encryption and the need for selective access to the image data is presented in [8]. An interesting image specific cryptanalysis example is presented in [9], giving significant information in the aspects of security that should be considered specifically for the case of image data. Additional information on cryptanalysis techniques based solely on permutations and XOR operations is given in [10]. The benefits and difficulties of block based image encryption schemes are analyzed in [11]. The fact that seemingly simplistic approaches, such as XOR masking of the image pixel data, may provide reliable encryption solutions depending on application requirements is pointed out in [12], [27], [28]. A particularly ambitious scheme for expert system based determination of the regions of interest of an image is presented in [13]. Permutation based encryption schemes targeted specifically to video images are presented in [14]. Selective encryption is another open topic appearing in literature. A selective encryption technique, suitable for directly encrypting compressed MPEG images is developed in [15]. The interaction between image compression and image encryption is analyzed in [16] and a method for bandwidth reduction via batch processing of correlated images, such as those found in video, is proposed. A significant drawback of standard security analyses for image encryption schemes is the lack of objective measures that have proven significance for the cryptanalytic resilience of such schemes [17]. Such objective measures are the object of current research [17]. The use of COTS smart phones by tactical edge users is seen by modern military as a means of promoting the situational awareness of this class of users that are frequently information challenged due to lack of secure communication channels [23]. This lightweight but robust encryption scheme addresses the problem of protecting the image Data-in-Transit [23]. Additional protection is of course needed for Data-At-Rest or In-Processing [23]. The overall development aims to promote the goal of exploiting COTS software, hardware and network infrastructure for the purpose of improving war and peace time tactical communication capabilities [24].

The paper is organized as follows. Section 2 gives an extensive account of the problems arising when attempting to design cryptographic protection for image transmission systems. The different requirements and compromises dictated by different applications are presented. Specific attention is given to the particular constraints imposed by the necessity for transmission of the images. Additional constraints due to computational resources are also examined. A detailed specification of the requirements from such cryptosystems is hence deduced. Section 3 describes the proposed approach for solving the problem, with particular emphasis on the scalability of the solution so as to match diverse set of cases. Additionally, issues concerning the selection of regions of interest and the application of error detection and correction techniques are also addressed. The proposed scheme aims to promote the level of security offered by portable COTS devices and hence promote the usability of such devices by field personnel in tactical operations. Section 4 presents a first approach to the cryptanalytic assessment of the proposed solution. Considerations concerning merit of cryptanalytic attacks on encrypted image transmission systems are first presented. The plaintext, approximation and a number of statistical and image specific cryptanalytic attacks are hence considered and an initial assessment of the resilience of the proposed system against such attacks is attempted. Finally conclusions are drawn and directions for future work are given.

2 Description of the problem

Image signals may vary dramatically in the resolution they carry, the rate at which data becomes available and the level of security they necessitate. Indeed, a medical image may be of high resolution, all of which is required to be encrypted and stored so as to satisfy the legal personal data protection requirements. A movie transmitted for recreational purposes via a subscription television service at high definition quality, produces large amounts of data at an extremely high rate but it is just required that unauthorized persons are incapable of viewing the images at their best quality.

On the other hand, imaging data coming from a field camera or facsimile images may be of low resolution, may contain large redundant areas (e.g. the white area of a page or the background of an area under surveillance) and the most difficult to achieve requirement is encrypting this information and transmitting it using channels that are likely to corrupt it. A small amount of corruption that would be acceptable in unencrypted transmissions, will lead to the total loss of data if security is also required. Consider for example the paradigm of a fax transmission. If in a plaintext fax a few bits were corrupted, this would lead to a few extra dots appearing in the page. Most users would hardly notice this happening. If however same the number of transmission errors happened in an encrypted transmission, depending on the encryption principle (block based and block size), the entire image might be lost. This problem may in some cases prohibit the use of secure channels for communication and hence jeopardize the efficiency of critical or sensitive operations, such as military operations.

The study of existing literature, presented in the previous section has demonstrated that, even though image encryption has been extensively studied, the case of extremely low color depth images has not been tackled. This study focuses on low depth images that carry critical information that is short – lived. Furthermore, the transmission is to be made in situations where neither the bandwidth nor computational resources are unlimited and the absence of transmission errors may not be assumed. In such cases it is common practice not to use any cryptography at all, since doing so would be impractical. This study proposes the introduction of a cryptographic algorithm that is lightweight enough for enabling utilization, while it is strong enough so as to render the decryption of the data by the adversary, within its useful lifetime, impractical. This problem is of particular importance to military applications, in the case of transmission of images concerning orders that are to be executed imminently. In this case the adversary might not know what the friendly forces are planning, but is going to be able to observe their actions within a very short period of time. Depending on the occasion, this could be of the order of hours, minutes or even seconds. As an example, consider a military unit that is about to be attacked by enemy forces. Their headquarters may wish to convey visual information concerning the approach of the attackers, or the required defense tactics. The enemy might already know or is about to find out this information respectively in each case, but it may prove of significant advantage for the friendly forces, if this happens after a significant time delay. Additionally, the algorithm is required to be such that, it can be practically implemented using normal, dispensable battlefield equipment, that is preferably COTS, while it cannot be cryptanalyzed, within time limits that are useful for the enemy, using equipment that the enemy would be willing to transport, install and maintain for this purpose.

This research is particularly focused on applications where low resolution and low color depth images are sufficient for the required performance. Typically in such cases both the bandwidth available for storage and transmission will be limited and the computational power that can be devoted for the cryptographic calculations will be severely restricted. In this context, the standard features desirable in any cryptosystem (as outlined and analyzed in [1]) may be interpreted as follows:

- Complexity: In such applications, computational power should be considered as being severely limited. Resources should ideally be uniquely directed to the Regions Of Interest (ROI's) of the image. Real time operation is desirable, but could in cases be slightly circumvented, as for example in the case of surveillance picture frames that could be updated less often than normal television frames.

- Compression efficiency and Bandwidth expansion: Possibly the most difficult goal to satisfy. Compressing the data too much creates processing overhead while not compressing data enough will adversely affect bandwidth restrictions. The answer may only be given on a per case basis, taking into consideration the particular hardware capabilities.
- Perceptibility: In general, the applications this research focuses on are security targeted and hence no level of leftover perceptibility of the encrypted image is acceptable. In contrast to examples like pay TV, in secure storage or transmission problems any perceived part of the image leaks information to potential cryptanalysts.
- Format compliancy: If an encryption process produces data that is compatible to the format of the plaintext data one encounters in the same application, this means that the encryption block may be introduced as an add-on feature to existing systems. This could prove particularly beneficial for the penetration of the technology.
- Error resilience: Depending on the type of application, some error resilience may be mandatory. This is especially true for applications where transmission is involved, since in general the existing infrastructure might not necessarily provide error-free data communication services.
- Adaptability, scalability and multi-level encryption: Given that the previous requirements are satisfied, possible adaptability of the algorithms to the capabilities of different devices that may be simultaneously operating in the same network is desirable. Adapting image quality is not applicable in general, since typically images will be binary. Hence, in most cases, all users will require to be able to process the entire image.
- Content agnosticity: The encryption process should be able to compensate for variations in the incoming image statistical properties.

At this point it should be clarified that the problem which the focus of this work was not the improvement of the compression rate of existing algorithms. The aim was to develop reliable encryption algorithms, given the compression of existing image encoding techniques used in various applications (tiff, jpeg etc). The level of security achieved by these encryption algorithms was also the object of investigation. The following section describes an encryption process that satisfies the requirements and solves the problems that have been described for the case of low color depth images.

3 Proposed approach

The approach tested in this study combines a linear and a non linear encryption scheme in order to ensure that information remains protected, while the exposure to transmission errors does not endanger but only small areas of the useful image. The work presented here is extending the method presented in [19], so as to increase security without losing the suitability for COTS based deployment. Furthermore, a recently proposed error detection and correction scheme [20] is applied that increases the reliability of the essentially unreliable channel.

Regions of interest (ROI) are determined by a very strict approach. The ROI determination algorithm is based on the facsimile transmission paradigm. A typical image following this paradigm is shown in Figure 1.

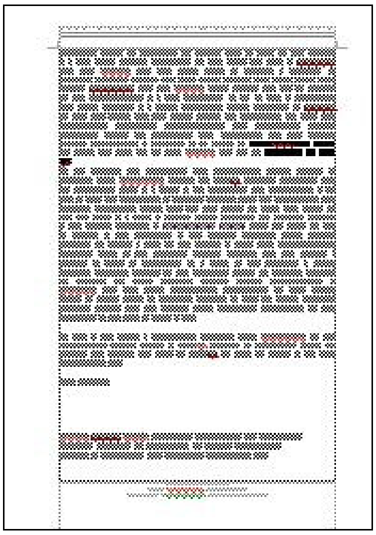

Figure 1. Typical Facsimile page form

The image may be assumed to be systematically laid out in rows. The scanning for ROI's is therefore carried out on a row by row basis. The pixels corresponding to a full block are assembled and examined. Any block with a single pixel different from its background is considered to mark the onset of a new region of interest. Given a row of pixels

$\{p_i\}$, with $i \in [0,N]$, the decision criterion is given in Equation 1.

$$\min(i) : p_i \neq \underline{0} \qquad (1)$$

The end of a row is scanned backwards in a similar manner to find the end of the region of interest. The blocks of the region of interest are then passed on for encryption, while blocks outside the ROI bypass this stage. All blocks are required to be complete and no blocks are allowed to cross the boundaries of the row within which they start. This approach leads to bandwidth savings for the facsimile transmission paradigm. This is true because, a text page will typically produce large white areas around its borders that will be left unencrypted. Similarly, large in – text gaps will also produce savings in bandwidth.

Before attempting estimates of bandwidth gains achieved, it should be noted that bandwidth reductions in encrypted images are much more significant in absolute terms that corresponding reductions in plaintext images. A typical encrypted facsimile page has been measured in experiments to be 4 to 9 times bigger in size than the corresponding plaintext image, even though both may be encoded in the same format (e.g. jpeg). This is because the encrypted image will typically present little or no redundancy [4]. For a typical A4 page with margins of 2.5 centimeters, the minimum bandwidth gain can be calculated as 40%. However this number is misleading as it takes into account the printing margins, which are easily detectable. The most important bandwidth reduction results from the detection of white areas within the useful area of the page (paragraph margins, inter – paragraph gaps, title spacing etc). Even though statistics of these gains are difficult to estimate, due to their high variability, but a conservative estimate for a mean paragraph size of 10 lines and single spacing may be conservatively estimated at 7%. Variants of this approach may be designed for perceived text layouts differentiating from the one shown in Figure 1 (e.g. double column, floating text segments etc).

Despite the ROI selection, the letters and symbols still contain a large proportion of white space inside their boundaries, while they consist themselves of uniformly, or almost uniformly, colored areas. This is due to the nature of the image being processed (text), as well as the fact that the images are of very low color depth (typically binary). Encrypting such an image, would therefore typically still produce systematic patterns on the encrypted result that would easily, or even readily, be legible as symbols. A sample of the systematic patterns that may appear in this situation is shown in Figure 2. In this picture it is relatively straightforward to distinguish the digits O, 1 and 4 and the letter sequence “www”.

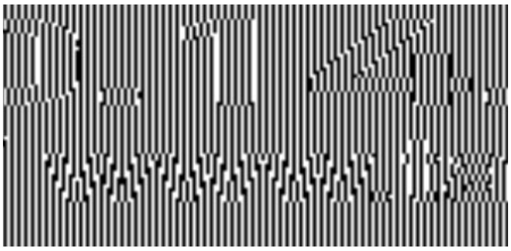

Figure 2. Sample systematic patterns appearing in encrypted segments

The encryption process therefore consists of two stages. In order to achieve reliable encryption, the data is first masked using random values originating from a pseudo random number generator and a linear masking function (XOR). Given a pixel sequence $\{p_i\}$ and a pseudo – random sequence $\{r_i\}$, the first stage cipher text $\{C_{1,i}\}$ will be obtained as shown in Equation 2.

$$C_{1,i} = p_i \oplus r_i \qquad (2)$$

The linearly encrypted data is hence encrypted with a block based non-linear algorithm, namely the AES. The block size and the key size of the AES have to be chosen in such a way as to maintain computational and bandwidth restrictions. Hence the second stage cipher text, given key k_i, is given as shown in Equation 3.

$$C_{2,i} = AES(C_{1,i}, k_i) \qquad (3)$$

A block diagram of the encryption process is shown in Figure 3.

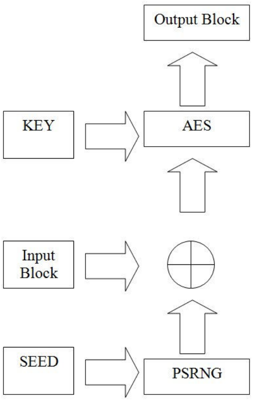

Figure 3. Block diagramof the stages of the encryption process

The polynomial of the random number generator is fixed while the seed changes in every line, according to a prearranged sequence of seeds, in a rolling manner. Additionally, the keys of the AES change between rows of the same transmission again according to a rolling key principle, thereby reducing the possibilities of cryptanalytic attacks such as the ciphertext only attack. In the results given in the following section, this was achieved via the use of tables of keys, pre – agreed between sender and receiver. It is planned for the final prototype to use a one time key. It should be noted that the key to the process is composite and consists of the AES key sequence, the PSRNG polynomial and the PSRNG seed sequence. As it was detailed above, the two ends of the communication channel need to be able to maintain and share those keys. The problem addressed by the proposed algorithm involves mainly portable devices to be used by personnel temporarily away from base for missions. It is therefore practical to implement the pre – agreement of keys based on a operational model of loading the device with enough keys before each mission.

For the results considered for this paper, block sizes of 8, 16 and 32 pixel values were used. A useful block is fed into the AES module with a key size of 256 bits, padded with non-significant data, as shown in Equation 2. Using a larger block size reduces the bandwidth necessary, while smaller sizes imply a higher level of security.

As it is apparent from the above description, the AES is implemented for operating in the Electronic Codebook (ECB) mode encryption, which is the most suitable for the limited computational resource case. However, the principle drawbacks of the ECB mode of operation for image encryption [25] are alleviated in this implementation. The masking with the random sequence and the padding imply that the resulting cipher is not suffering from the lack of randomness that is the principle drawback of ECB [25]. Furthermore, since the padding data is pseudorandom, identical data blocks do not produce identical cipher blocks, making the scheme unsusceptible to replay attacks.

In order to maintain the format compliancy requirement stated earlier on, the encrypted blocks are reassembled into a valid image file. In order to reverse the process, the receiver will need to be able to synchronize with the seeds and keys used at the transmitter side. Due to the noise-like appearance of the cryptographic algorithm output, it is not possible to perform a detection process, reciprocal to the region of interest detection described earlier. Therefore, synchronization symbols had to be inserted at the beginning of each row in the final output. Given a row of pixels $\{p_i\}$, with n the determined onset of the ROI and m the determined end of the ROI, the insertion of the synchronization symbol requires the assignments of symbols shown in Equation 4, where $\underline{1}$ denotes a unit pixel (for bitmap a value of 1) and ≡ denotes assignment.

$$\begin{aligned} p_{n-1} &\equiv \underline{1} \\ p_{m+1} &\equiv \underline{1} \end{aligned} \tag{4}$$

These symbols do not inhibit the compliancy to the format of the data, which can still be perceived by any of the remaining processing elements of the system as a valid image file. Visually, these symbols appear as isolated dots on the image that could be ignored as unperceivable for the average application, or could be removed if this is necessary.

The use of error correction techniques as an enabling technology for robust secure image transmission has been proposed in literature [18]. A method was recently proposed for correcting transmission errors corrupting the data that could deal with both isolated and burst errors [20]. This method, which operates at a reasonable computational overhead, was used as an additional block enhancing the error resilience properties of the encryption scheme. The use of error correction schemes could be relevant even for a smart phone based implementation, in the case where transmission is based on tethering the device to radio equipment, or should be disabled in the case where 3G type networks are used.

Alternative encryption schemes involving non-linear Boolean transformations, such as those that the author has recently studied for user authentication purposes [21], are currently being investigated.

A simplified block diagram of overall the proposed approach is shown in Figure 4.

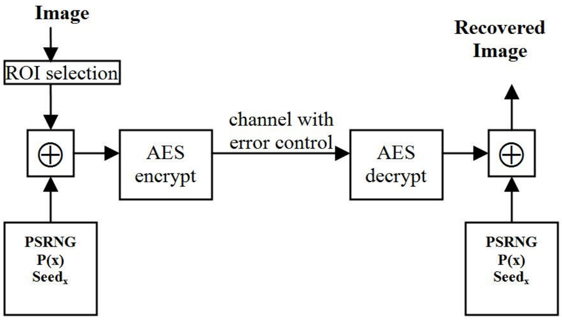

Figure 4. Block diagram of the proposed setup

The possibility of integrating advanced authentication and key management techniques (such are those presented in [22]) is being investigated. Additionally, advances in automated algorithmic design that are anticipated following the research in [21], are expected to enhance the overall security of the system, while reducing the required computational complexity, via the use of Boolean cryptographic functions.

The proposed encryption scheme was implemented in Matlab using C functions. The results of the simulation and cryptanalytic tests performed are given in the following section.

4 Cryptanalytic Assessment

Cryptanalytic attacks with particular significance for image encryption systems include the Known Plaintext Attack but also the Approximation Attack, the Error Concealment Attack and the Statistical Attack [1].

The proposed approach is meant to be useful for applications where the useful life of image data is of limited duration and where normally none or limited cryptographic protection would be used. This encryption scheme aims to maintain confidentiality and integrity of the data, without guaranteeing availability. Availability, especially in tactical situations, is an independent problem which is tackled by use of specialized communication channel infrastructure. Therefore, for the application paradigm, encompassing the conditions outlined above, a first approach to the cryptanalytic assessment of the scheme will be attempted. All analyses were made using the Matlab suite of tools.

4.1 Plaintext attack

In order to mount a known plaintext attack on an image cryptosystem, a cryptanalyst would try to exploit specific characteristics of the encrypted data in order to recover the encryption keys [1]. Such characteristics include the existence of file headers and frame markers, of smooth spaces in images and still frames in video. The proposed approach produces images that are format compliant, i.e. the file headers are there in plaintext format and correspond to the encrypted version of the data. They hence carry no information concerning the encryption keys that a cryptanalyst could exploit. Areas of the image that are smooth (white) are either left unencrypted or are masked with a random pattern before being encrypted. Given the rolling random seeds and the rolling encryption keys, such areas will convey no information about the encryption key that might be useful to a cryptanalyst. A mathematical proof for this statement is currently being developed and will be presented in a future publication.

4.2 Approximation attack

An approximation attack will try to detect any traces of perceptual information that are still visible after the encryption process, even if it is not possible to extract the exact original image. This is mainly achieved via exploitation of the spatial correlation in the image data [1]. This type of danger might be considered as extremely significant for the particular application considered in this research, given that scanned text might still be legible even if only a small amount of such correlation exists. Additional dangers will materialize if edge information remains in place after the encryption process. In order to investigate this type of attack, the correlation properties of selected areas of both encrypted and plaintext images have been studied. Figure 5 shows a sample portion of an encrypted image.

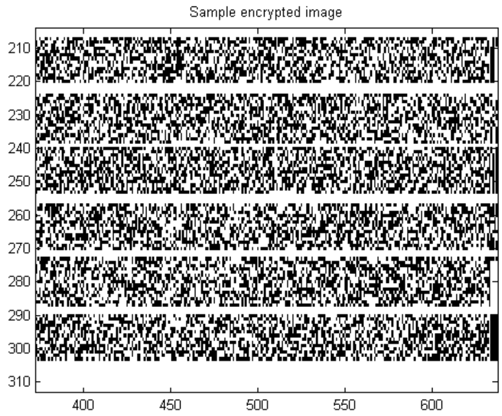

Figure 5. Example of an encrypted text image

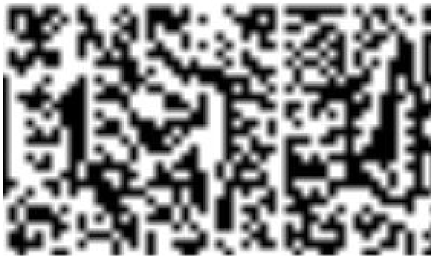

Figure 6. Detail of the encrypted image

The noise-like properties of this image are clearly visible. Figure 6 depicts a detail of a text segment, where all the systematic patterns of Figure 2 shown in the previous section have disappeared. Figure 7 depicts an attempt to apply edge detection (using the Sobel method) on the encrypted image of Figure 5. The result shows that there exists no apparent exploitable edge information in this example. The same conclusion has been drawn on several similar experiments with different images and different operators such as the Prewitt, Roberts, Laplacian and zero – crossing methods for edge detection.

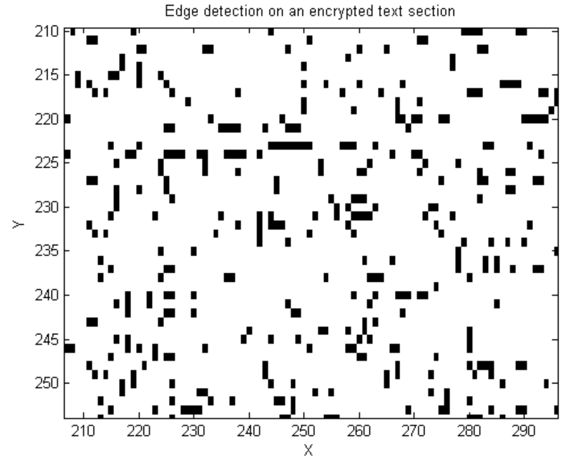

Figure 7. Sobel edge detection on the sample image

4.3 Error concealment attack

An Error Concealment attack would attempt to exploit statistical information and knowledge about the format of the data to achieve a perceptual cracking of the encryption [1]. Such an attack would be considered as successful, if the attacker managed to recover a recognizable version of the image, with inferior quality compared to the original [1]. In the case o this attack, the weak point of the ciphertext is redundancy left over after the region of interest selection and encryption processes, which may be exploited for revealing degraded but recognizable parts of the image [1].

In order to investigate the resilience of the proposed algorithm to such attacks, the correlation properties of the encrypted image have also been studied, both at large scale (image level) and at small scale (letter level). Correlation would reveal any similarity existing between the original image and the ciphertext image, as required by this type of attack in order to function. The result in Figure 8 shows the correlation of a 300x300 encrypted region with its plaintext version.

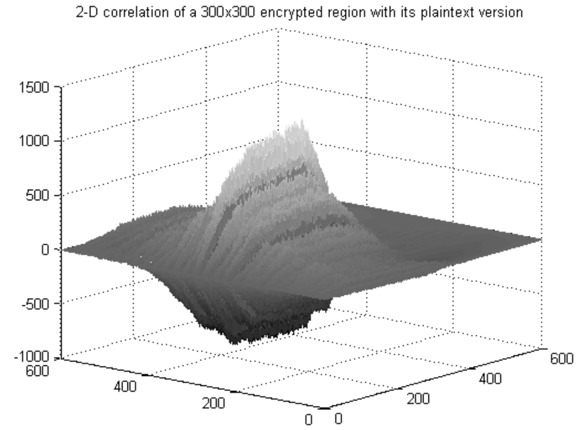

Figure 8. Correlation between encrypted and plaintext images

For the above calculation, the bitmap image has been normalized by subtracting its mean and hence contains negative values. A maximum correlation score of roughly 4000 is hence expected. The observed peak of approximately 500 should therefore be attributed to windowing effects rather than any real correlation between the data of the two images. Furthermore, the above correlation result should be compared with Figure 9 that shows the autocorrelation of the plaintext version of the same region and Figure 10 that shows the cross correlation of the encrypted region with another random encrypted region of the same dimensions.

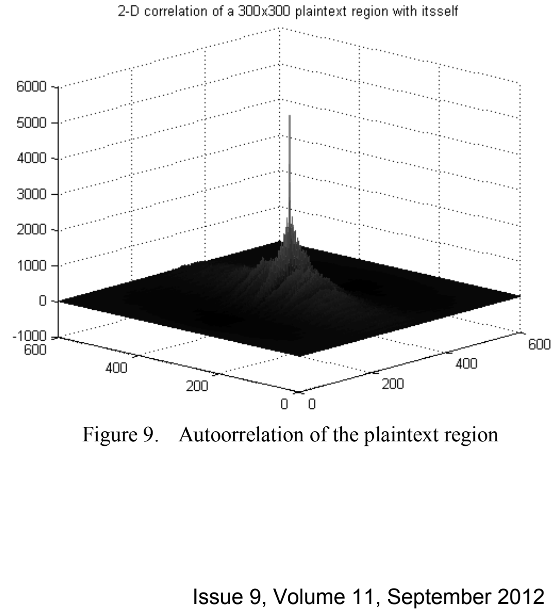

Figure 9. Autoorrelation of the plaintext region

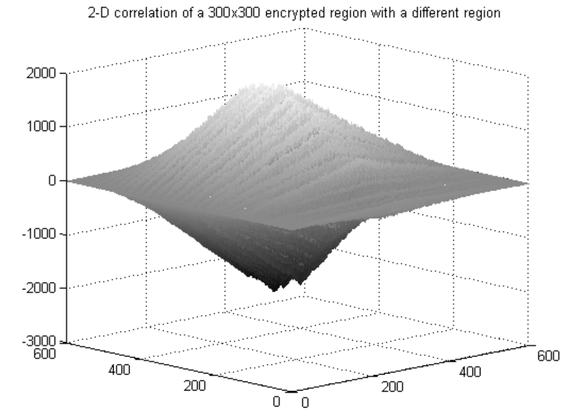

Figure 10. Cross correlation of the encrypted region with a randomly selected one

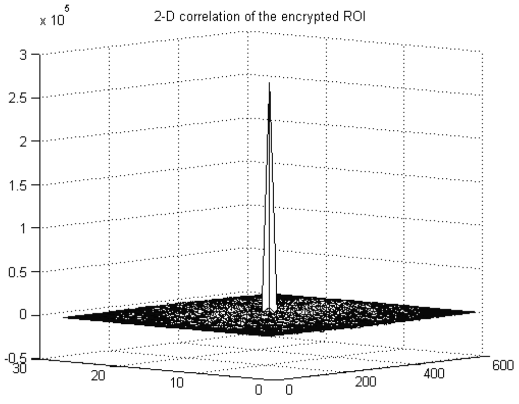

Figure 11. Autocorrelation of a ROI segment

From Figures 9 and 10, it may be concluded that indeed a high correlation score should have been achieved if there were indeed any leftover unencrypted exploitable information left in the encrypted image. The second conclusion that may be drawn is that the correlation score is independent of the area of the image that is being examined. Attackers are therefore prevented from managing to use known plaintext to mount either of the two above types of cryptanalytic attacks. Additionally, Figure 11 shows the autocorrelation of a segment of the encrypted image that corresponds solely to a region of interest segment of the image. The noise like behavior of the encrypted image is clearly observable. It should be noted that all the previous results (apart from Figure 11) have been obtained using areas of the image that correspond principally to useful data (areas in the middle of paragraphs containing small intermediate line spacing).

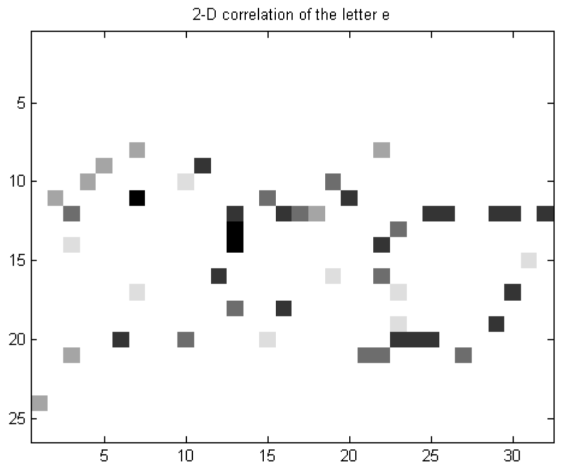

Figure 12. Cross correlation of the letter "e" with its neighbourhood

4.4 Statistical attack

A statistical attack on this particular cryptosystem would try to exploit the language redundancies that would cause the repeated appearance of common letters in the encrypted data. The cryptanalyst would exploit the predictability of a particular element of the image or relationships between the original bitstream and the cipher codestream [1]. Such relationships would lead either to recovering the plaintext without knowing the key or to substantially reducing the search space upon which a brute force attack may be mounted.

The conceptual elements in the case of the facsimile paradigm are the letters of the alphabet. In order to produce an initial assessment of the resilience of the proposed algorithm to such attacks, it was investigated whether it would be feasible to exploit linguistic and format knowledge in order to locate letters within the ciphertext.

Towards this aim, the area where the letter "e" lies in the encrypted image was separated and its correlation with various areas of the image was calculated. The results obtained at the area where this letter is actually located are shown in Figure 12. Similar results were obtained when examining other areas of the image. It should be noted that the letter "e" is a letter that appears with a high probability in the English language. The experiment was repeated with all letters of the alphabet. The conclusion drawn from the above experiment is that attempts to detect letters in the encrypted image are not successful.

4.5 Other types of attacks

Further quantitative analysis of the resilience of the proposed method to cryptanalytic attacks is under way and the applicability of quantitative measures like the Luminance Similarity Score and Edge Similarity Score [1] is being investigated, together with other objective security metrics such as those proposed in [17].

Summarizing this initial cryptanalysis assessment and considering the combination of linear and non-linear cryptography that the proposed method uses, the small block size appears as an advantage against cryptanalytic attacks. If a particular block were to be jeopardized, then the limited amount of data that would become available to the attacker would be insufficient for reducing the random sequence used. Furthermore, the masking of the data via the use of the random sequence essentially makes the operation of the AES more effective, since there exist no more white areas where there is a risk for repetitive patterns carrying information to leak out of the encryption process.

The proposed scheme exploits the fact that the images for encryption are of low color depth, in order to employ the simplistic region of interest selection technique described in Section 3 above. Extensions may be envisaged that may be applied to higher color depth images, e.g. by serializing the corresponding bits, provided that the short lifespan of the information prerequisite continues to be maintained.

This technology is consistent with the current trend of using COTS systems for military applications in order to minimize the ever increasing costs of development [23], [24]. The principles of this approach are that COTS technologies are evolving far more rapidly than military technology may ever evolve, since the funds available for military research are being constantly reduced. Furthermore, this equipment requires shorter training periods for military staff than purpose built field equipment, since especially younger personnel, are extremely familiar with its operation. In this spirit, COTS smartphones are being deployed for battlefield use. Such devices are powerful enough to apply the proposed scheme to significantly more complex images, such as content enhanced COTS territorial maps, such as Google maps. An Android phone prototype implementation of the proposed scheme is currently being developed, that will be used for more thorough testing and evaluation.

An open issue remaining to be investigated is the case where the device implementing the algorithm is captured by prospective attackers. The requirement is in this case that future communications are not jeopardized because of this fact. This problem is currently being investigated. A partial solution, concerning the protection of the AES block, was presented by the author and associated researchers in [26]. This solution’s applicability however, depends on the physical circuit layout of the device being used and its ability to be connected to additional elements such as smart cards. Other COTS technologies, such as screen locks, pins and passwords, may also contribute towards this aim, combined with more specialized countermeasures. These countermeasures may include mechanisms for merging the memory contents or honey pots that are activated when user authentication fails [23], [24].

5 Conclusion

A study of encryption of digital image data has been presented. The particular nature of the problem of encrypting image data that is intended for transmission or storage was analyzed. This problem was studied in the broader context of facilitating the exploitation of COTS technology and networks, for the benefit of tactical level military users. A review of the state of the art of image encryption in current literature was given and the fact that many issues still remain open was concluded. The problem and particular requirements from image encryption schemes that deal exclusively with encrypting low color depth images are extensively analyses and the applicability of standard image encryption requirements to this particular problem is extensively investigated.

An encryption scheme is proposed that is intended for providing secure and robust transmission of encrypted images over channels permitting errors was proposed. An initial cryptanalysis study for the proposed scheme was presented that demonstrated satisfactory robustness properties against common attacks. Further work is currently under way in the fronts of introducing more secure encryption algorithms in the scheme, of further reducing the computational effort required for the encryption process and of selecting relevant objective security metrics and applying them to better assess the resilience of the scheme to attacks.

An analysis was made for applications of the proposed scheme to COTS communication equipment intended for battlefield use. The advantages and drawbacks of such applications was considered.

References:

[1] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A brief overview" *Rec. Advan. in Mult. Sig. Process. and Commun., SCI 231*, pp. 417–449, 2009

[2] S. Lian, D. Kanellopoulos and G. Rufo, "Recent Advances in Multimedia Information System Security", Informatica 33 (2009) pp 3–24.

[3] W. Fang and J. Lin, "Multi-channel Secret Image Transmission with Fast Decoding: by using Bit-level Sharing and Economic-size Shares," International Journal of Computer Science and Network Security, vol.6 No.5B, pp 228 – 234, May 2006.

[4] D. Xie and C. Jay Kuo, "Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream," EURASIP Journal on Information Security Volume 2007, Article ID 35262, 18 pages, 2007.

[5] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives," EURASIP Journal on Information Security Volume 2008, Article ID 179290, 18 pages 2008.

[6] M. Younes and A. Jantan, "An image encryption approach using a combination of permutation technique followed by encryption": International Journal of Computer Science and Network Security, VOL.8 No.4 pp 191 – 197, April 2008.

[7] I. Atakli, Q Wu, Y, Chen and S. Craver. "BLINK: Pixel-Domain Encryption for Secure Document Management" MM&Sec '09 Proceedings of the 11th ACM workshop on Multimedia and security, pp 171-176, 2009

[8] C. Fonteneau, J. Motsch, M. Babel and O. D´eforges. "A Hierarchical Selective Encryption Technique in a Scalable Image Codec". In International Conference in Communications, Bucharest, Romania, 2008, http://hal.archives-ouvertes.fr/hal-00336403/

[9] S. Li, Chengqing Li, K. Lo, and G. Chen. "Cryptanalysis of an Image Scrambling Scheme without Bandwidth Expansion. IEEE Transactions on Circuits and Systems for Video Technology, VOL. 18, NO. 3, PP. 338–349, 2008

[10] M. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm": International Journal of Computer Science, VOL. 35 No. 1, February 2008.

[11] J. Hu, F. Han. "A pixel-based scrambling scheme for digital medical images protection". Journal of Network and Computer Applications 32, 788–794, 2009

[12] A. Wong and W. Bishop. "Expert Knowledge Based Automatic Regions-of-Interest (ROI) Selection in Scanned Documents for Digital Image Encryption" Proceedings of the 3rd IEEE Canadian Conference on Computer and Robot Vision, 2006

[13] D. Socek. "Permutation-based transformations for digital multimedia encryption and steganography." PhD Thesis, Florida Atlantic University, 2006

[14] M. Droogenbroeck and R. Benedett. "Techniques for a selective encryption of uncompressed and compressed images". Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 9-11, 2002

[15] D. Arroyo, C. Li, S. Li, G. Alvarez and W.A. Halang. "Cryptanalysis of an image encryption scheme mased on a new total shuffling algorithm" Chaos, Solitons & Fractals, Volume 41, Issue 5, 15 September 2009, Pages 2613-2616

[16] T.H. Chen, C.S. Wu. "Compression-unimpaired batch-image encryption combining vector quantization and index compression". Information Sciences 180 1690–1701, 2010

[17] J. Sun, Z. Xu, J. Liu and Y. Yao. An objective visual security assessment for cipher-images based on local entropy. Multimed Tools Appl 53:75–95 2011

[18] M.A. El-Iskandarini, S. Darwish, S.M. Reliable wireless error correction technique for secure image transmission., 2009. 43rd Annual 2009 International Carnahan Conference on Security Technology, pp 184 – 188, 2009

[19] N. Doukas and N.V. Karadimas. A blind source separation based cryptography scheme for mobile military communication applications. WSEAS Transactions On Communications , Volume 7 Issue 12, pp 1235-45, 2008

[20] Bardis, N.G, Markovskyi, O., Doukas, N. Efficient burst error correction method for application in low frequency channels and data storage units. IEEE Digital Signal Processing (DSP), 2011 17th International Conference on, 2011

[21] Bardis, N., Doukas N. and Markovskyi, O. 'Fast subscriber identification based on the zero knowledge principle for multimedia content distribution', To appear in the Int. J. of Multimedia Intelligence and Security.

[22] Nikolaos Bardis, Nikolaos Doukas, and Konstantinos Ntaikos. 2008. A new approach of secret key management lifecycle for military applications. WSEAS. Trans. on Comp. 7, 12 (December 2008), 2011-2021.

[23] A. M. Buibish, N. E. Johnson, D. Emery and M. Prudlow. Cryptographic Solutions for COTS Smart Phones. Military Communications Conference (MILCOM) 2011 , Page(s): 1434 – 1439

[24] R.S. Oregon. Smart Fires: A COTS Approach to Tactical Fire Support Using a Smartphone. PhD Thesis, Naval Postgraduate School, September 2011

[25] Wikipedia: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

[26] Bardis, N.G.; Doukas, N.; Markovskyi, O.P.; , "Organization of the polymorphic implementation of Rijndael on microcontrollers and smart cards," Military Communications Conference, 2010 - MILCOM 2010 , vol., no., pp.1783-1787, Oct. 31 2010-Nov. 3 2010

[27] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image Encryption Process Based on a Chaotic True Random Bit Generator", In Proc. Of 16th IEEE International Conference on Digital Signal Processing (DSP 2009), Vols. 1 and 2, pp. 1091-1094, July 2009, Santorini, Greece.

[28] F. Neri, Software Agents as A Versatile Simulation Tool to Model Complex Systems. WSEAS Transactions on Information Science and Applications, WSEAS Press (Wisconsin, USA), Issue 5, Vol. 7, 2010, pp.609-618.