International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 8, Issue 3, 2019

# Compatible Information Security System for Electronic Human Resource Management Encryption

**Zubaidah Abdulhakeem Majeed[a], Ahmed Nashaat Shakir[b*], Murad Bahram Khorsheed[c],** [a,b]Department of Dormitories, Presidency of the University of Kirkuk, Kirkuk University, Kirkuk, Iraq, [c]Department of Statistics, College of Administration and Economics, Kirkuk University, Kirkuk, Iraq. Email: [a]ahna2005@uokirkuk.edu.iq, [b*]zubaidah.abdulhakeem@uokirkuk.edu.iq, [c]muradbahram@yahoo.com

This work was an attempt to study and characterise compatible information security system involving electronic human resources management (E-HRM): as a part of internet environment dealing with tremendous amounts of confidential information such as personal information of employees within an organisation or vital documents involves work such as financial and technical details of certain products. The proposed solution was implemented taking into consideration the essential assumption; that the confidential information was unchangeable, so employees in general do not have permission to adjust it, therefore this work handled these information as images. The second vital assumption was that the tremendous amount of data belonging to electronic human resources management cannot be handled using conventional (sequential) encryption. Instead it should be divided into blocks. So this work used counter-mode operation to solve this problem and to save more time via parallel operation quality. Security keys were generated using Hénon and Lozi maps. The proposed model provides adequate levels of information security against cyber attacks such as brute force and letter frequency attacks.

**Key words:** *A Confidential Information, B Cybercriminals, C Hénon and Lozi Maps, D Encryption, E Security Key Generators.*

## Introduction

The management framework has a lion share in the development of any organisational environment. Human Resources Management (HRM) is an important part of the entire management system. HRM has been a high priority when evaluating the performance of diverse organisations, especially those with large scale systems (Xing et al., 2016; Zibarras and Coan, 2015). With tremendous development in Information Technology (IT): which deals with various data forms such as text and images, it is indispensable quality for any management system utilising such state of the art technologies to develop new style of management, based on websites. Therefore, the conventional HRM switched to a new one (E-HRM ) Electronic Human Resources. This new environment provides more reliability and activity for communication between managers and employees, taking into consideration the tremendous amount of data which exceeds gigabytes, so higher degree of compatibility involves handling such data became essential requirement to ensure high performance for all individuals within entire management system (Jensen-Eriksen, 2016).

The main task of E-HRM is to achieve this compatibility, by utilising IT for networking and enhancing the capacity of human resources (managers and employees) to share their data (text, images, videos) so as to improve a comprehensive performance of organisation and saving more time and money. Hence , the latest management systems in different fields have given much attention to E-HRM, especially economic organisations dealing with large numbers of people and systems; time and money are main constraints in such competitive environments (Bissola and Imperatori, 2014).

## E-Hrm Classification

The current E-HRM can largely be categorised into three groups, according to users' goals:

a) **Operational E-HRM** : it focuses on utilising technology within administrative functions , for instance payroll and employee personal data. Operational e-HRM enables employees to maintain their personal data via up-to-date websites from their organisation.
b) **Relational E -HRM** : it assists individuals to boost their relationships via IT in different activities, such as online training, discussions and the exchange of opinions.
c) **Transformational E -HRM** : many organisation attend to short and long term goals; this model provides adequate opportunities for management systems to prepare individuals with high qualifications, crucially through the web-based tools of any organisation (Strohmeier and Kabst, 2014).

**Challenges of Switching From Conventional Hrmto E-Hrm**

As aforementioned EHRM is essential to any organisation. However, switching from conventional to new forms based on IT capabilities has been challenging, requiring careful study before this style of management is adopted. These challenges include assessment of individuals by Human Resources (HR) and in their technical aptitude, executing a new service delivery model; computerising work processes; rearranging the HR organisation; assigning new criteria for HR constraints; and implementing HR technology support (Strohmeier, 2014).

The most vital constituent of an organisation is its employees. Therefore the attitudes of employees in terms of E-HRM will, in the long-term, contribute very greatly to maximising success and developing this type of management. Here, the chiefs of departments in an organisation can play a key role in familiarising individuals with their with new environment (E-HRM). The breaking of barriers to new technology depends on departmental chiefs and organisational heads in general. At the beginning, it is normal that individuals face obstacles and difficulties, but with continuous encouragement their incentives will increase and they get involved in the new situation (Bondarouk et al., 2017).

**E-Hrm and Security Challenges**

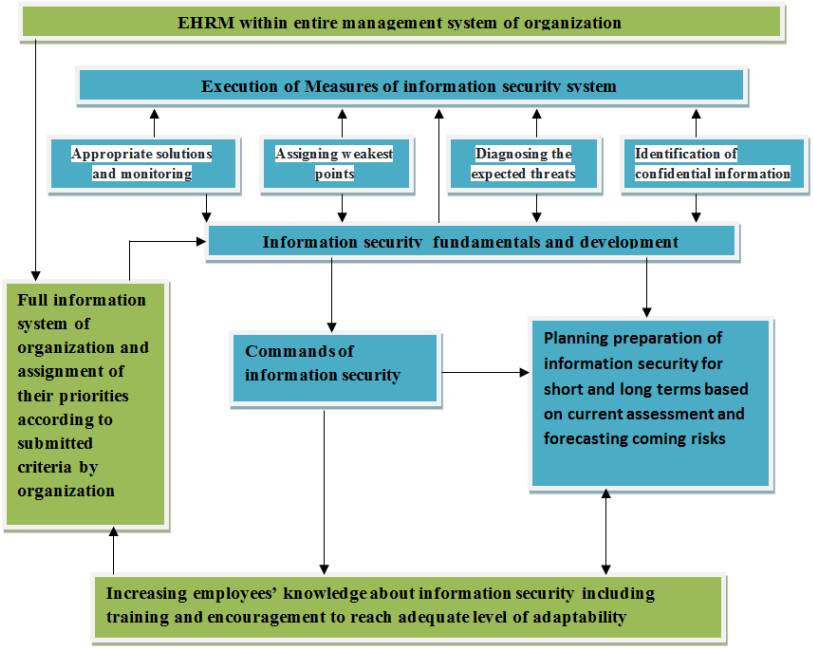
Because EHRM is part of IT for any organisation, normally it faces security challenges permanently. Huge amounts of individuals' information might be under attack from cyber-criminals, so it is crucial to minimise opportunities for unauthorised access, the revelation of information, and the illegal changes to information. This information documents confidential documents for individuals and entire organisation. It should be extremely secure. Achieving a high level of information security for any organisation is difficult, because the tools to make information highly secure must also allow adequate access for individuals seeking this confidential information (Kulkarni, 2014).

The success of any security system has been built on three phases; first, identification of confidential information; second, diagnosing the expected threats; third, assigning the weakest points in a security system, to finally making decisions to select appropriate solutions, and continuous monitor them to perform evaluations of the security system used. Information security like other disciplines has executive measures, such as passwords, firewalls, encryption, antivirus software, legal liability, and security knowledge. Diverse types of information security threats might occur. Currently software attacks are most common and dangerous. Others such as intellectual property stealing, and identity stealing are also prevalent. Users worldwide suffer very dangerous software attacks such as viruses and Trojan horses (Jain and Goyal, 2014). Intellectual property theft and identity theft

have focused on seizing users' personal information, then using it to obtain confidential information. The rapid development of communication systems and the very large scale of internet applications, via computers and smart phones, have maximised the chances for attacking users` information, so currently organisations from governments to low-level organisations spend huge budgets on information security (Kim, 2016).

The economy's financial and commercial foundations consider information security a backbone of its enduring, high level of success in competitive environments, by securing information for employees, customers, investors, and product quality, as well as long-term goals under study. E-HRM deals with offline information (saved on hard disk) and online information on the internet via different applications, for instance emails and social media. Therefore it requires a high level of coordination between information security staff, internet service provider, security management and parties who possess information systems. The integration between E-HRM as a part of management systems of organisation, and information security systems, has required defining the full information of organisations submitted by management system to information security systems, to continuously assess the performance of security measures. The proposed Figure (1) fully expresses the abovementioned integration.

**Figure 1.** Integration between EHRM and information security system



## Problem Statement and Proposed Solution

### *Introduction*

Organisations in diverse fields worldwide deal with giant volumes of data (information) which sometimes exceeds gigabytes or terabytes. Information in different patterns such as images and text are exchanged daily within individual organisations and with others; therefore information security systems address very complex situations. That requires high levels of security, and the quality of security measures, to be central when building successful information security systems. Encryption is a vital security measure applied commonly in communication systems. The framework of encryption can be described in encoding the confidential information of individuals or entire organisations with an appropriate technique, to enable only authorised parties, for instance employees and managers, to access them and on the same time tightly prevent any third party from reaching them.

In conventional encryption procedure, the confidential information defined as plaintext has been encrypted via one encryption algorithm, defined as cipher, to generate 'ciphertext' at the transmitter side, while at the receiver side the ciphertext has been decrypted to extract this information. To perform security goals, encryption and decryption processes have been implemented by using security key based on random behaviour of mathematical function such as pseudo random which is considered a common key generator used in the software of security applications. Security keys have been classified into two types according to the nature of the application. The first key one is a symmetric key. In this case the same key is used by both encryption and decryption processes. The second is a public key. In this case the security key can be allowable for any user (sender) within an organisation, to perform encryption whereas the receiver is authorised to read information only.

In the present work, two assumptions were considered as providing adequate levels of information security for any organisation. The first one is considering the confidential information of organisation including personal information of individuals, financial documents involve work such prices or technical details of products as are unchangeable. In other words employees are not permitted to adjust such documents. Therefore this information is handled as images, to ensure minimum security requirements, and to face cyber attacks which depend on the frequency analyses of ciphertext which count letters if the confidential information were sent as text, and try to detect the hidden information. The second issue is the colossal amount of data lead to avoid conventional encryption techniques to others take into consideration such large volume of information. Thus, it is an indispensable requirement that block cipher modes of operation are based on division data (confidential information) in blocks, facilitating their use. A block cipher is appropriate for encryption or decryption processes based on one fixed-length set of bits called a block. A

mode of operation illustrates how to frequently apply a cipher block technique, to ensure the secure transition of huge data through a block. General modes of operation involve an initialisation vector (IV): which is an exclusive binary chain and essential for every encryption process. The IV should be non-duplicating and, and it may be random (Pramanik et al., 2019; Fay, 2016; Taha et al., 2019; Mahdi et al., 2019).

The initialisation vector ensures that dissimilar ciphertexts are obtained when the same plaintext is encrypted many times separately with the one key. Block ciphers are perhaps competent for use on diverse block sizes, however, during transition the block size is always unchanging. Block cipher modes run on entire blocks and necessitate padding the last part of the data to a complete block, if it is minor than the present block size. Padding is additional to the opening, middle, or ending of confidential information processed by encryption. There are many modes of cipher operation. Each has aspects and drawbacks , however Cipher Block Chaining (CBC) is its most common mode. However, in this work it was not used because of its sequential operation mode. In other words, the encrypted information should be padded to a multiple of the cipher block size.

The present research was based on Counter Mode operation (CTR). This mode has random access quality which saves more time when handling information unlike CBC. CTR mode is more fit to meet parallel operation requirements on more than one processor. Moreover, this technique has not experienced the short-cycle issue. Under this mode the initialisation vector (IV) is a counter. The length of counter and plaintext should be equal to perform encryption processes. The mechanism of CTR is the encryption value of a counter using security key (K): then the output of encryption will be XORed plaintext (P) to obtain ciphertext (C): and in decryption mode at receiver side ciphertext (C) will be XORed that output to obtain plaintext (P). In this work the security keys were generated by two chaotic discrete functions, to achieve the high level of complexity that will minimise the chances of an attacker breaking a proposed security solution.

Chaotic discrete functions are highly sensitive to minor changes in the initial condition. Thus, even very simple changes will alter the output of such functions. This outstanding behaviour of chaotic systems occurred in diverse natural and imitation systems in many disciplines, such as economics and engineering applications. The chaotic discrete functions were used as key generators in this work are Hénon and Lozi maps.

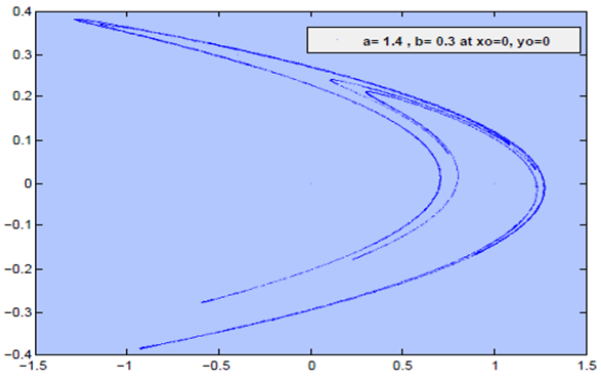
***Mathematical Behaviour of Used Key Generators***

The mathematical model of a Hénon Map had been submitted in (1976) as a two-dimensional function. Equation (1) describes this map which contributed greatly in characterising,

mathematically, discrete dynamic systems experienced from the special response. Figure 2 illustrates obviously random behaviour in this map.

$$X_{n+1} = 1 - aX_n^2 + bY_n \ldots\ldots\ldots\ldots\ldots (1)$$
$$Y_n = bX_n$$

**Figure 2.** Conventional Hénon Map

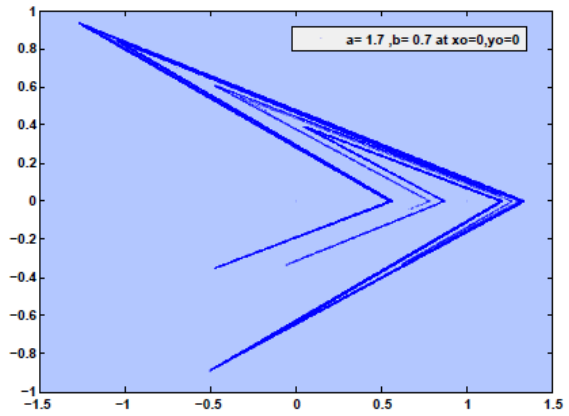



Equation (2) shows another outstanding random response of a Lozi map, submitted in 1978. Lozi mathematical models have been implemented in diverse disciplines such as control systems, synchronisation theory and secure communications. Figure (3) shows random behaviours of a Lozi function.

$$X_{n+1} = 1 - a\left|X_n\right| + bY_n \ldots\ldots\ldots\ldots (2)$$

$$Y_{n+1} = bX_n$$

**Figure 3.** Conventional Lozi Map



It is worth mentioning that the 'a' and 'b' parameters greatly influence the shape of the random response for both functions (Khan and Shah, 2014; Alpar, 2014).

***Procedure of Proposed Solution***

Based on the above assumptions, confidential information is considered an image in this work. The two key generators will be responsible for generating security keys (random numbers). Therefore these numbers should be transformed into an integer number and put in order from 0 to 255, to express the intensity value of each pixel inside plaintext (image). The transformation process needs an absolute sequence function, to avoid negative values, each ($X_n$) multiplied by 1000. Then the output numbers are normally real, so floor functions should be used to obtain integer values. Equation (3) shows the entirety of this step:

$$Z_n = \lfloor \| X_n \times 1000 \| \rfloor \; \ldots\ldots\ldots (3)$$

$Z_n$ represents the output integer number and final value of a generated security key, by Hénon or Lozi maps which will be used as (K) in the (CTR) operation. The counter will start from zero to a maximum value 255. Figure (4) illustrates a full proposed security solution including encryption and decryption conditions. The quality of parallel operation is obvious; a user can process many forms of information within a specific time. The huge amount of information for any organisation is not less than the tremendous number of daily gigabytes. For instance the number of employees in an organisation is 100, each one deals with 100 megabytes. Therefore the whole volume of data (information) is about 10 gigabytes, which might be online often. Thus, there is a very high threat that users lose part or the whole of their confidential information. For study purposes, and based on the above mapping, the length of key and plaintext is 8 bit, and the number of encryptions and decryptions is four processes (four blocks subjected to a process at the same time). The level of complexity will be very high in practice, when the usual length of the counter and plaintext block is 64 bit or 128 bit. A brute force attack will need more time to reveal the confidential information, and the complexity will be higher if the plaintext (image) is processed by the amount of noise.

**Figure 4a.** Proposed Encryption System Based on Advanced CTR

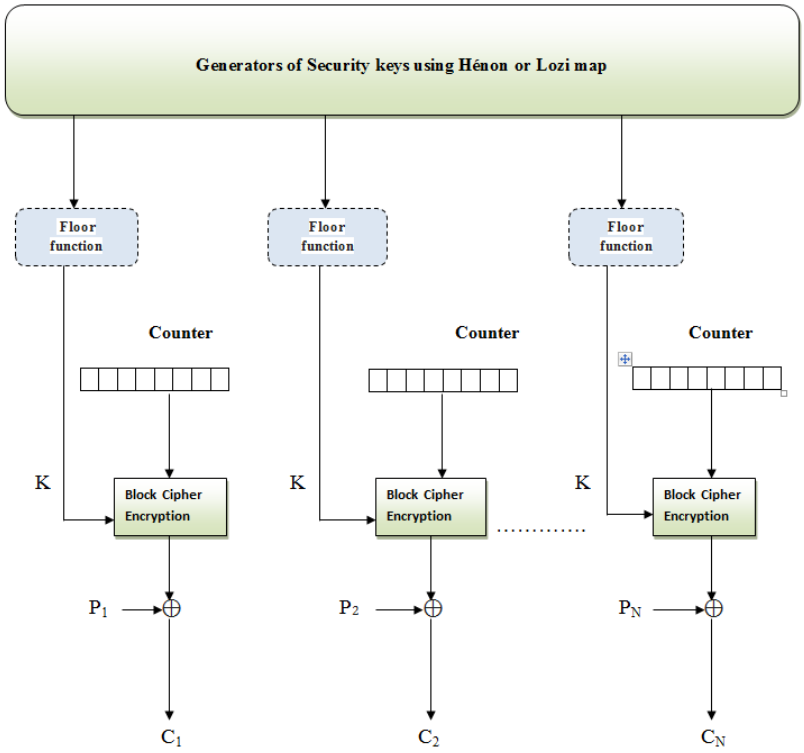
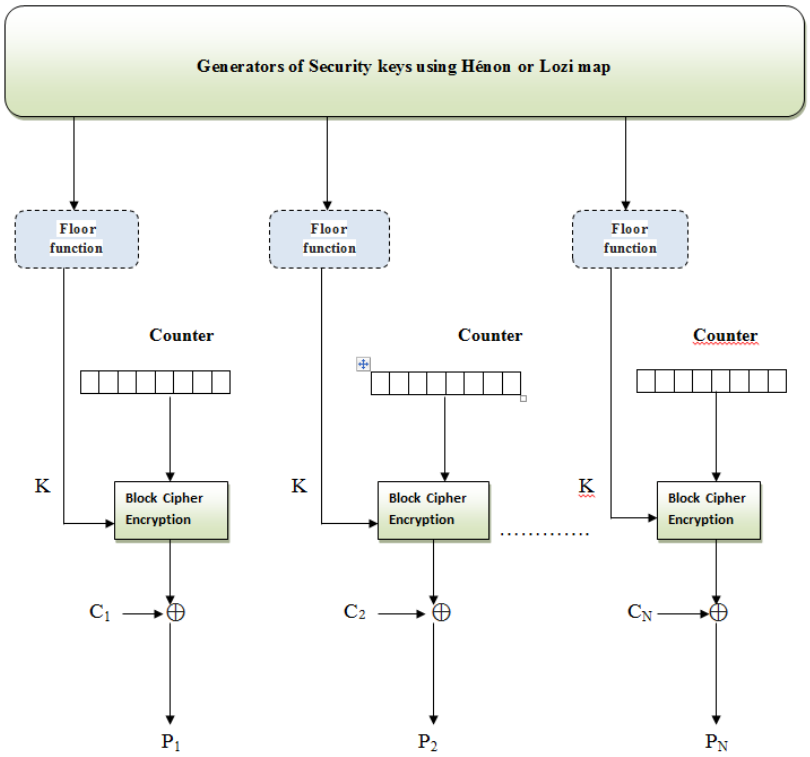



**Figure 4b.** Proposed Decryption System Based on Advanced CTR



***Results and Discussion***

The computer used to obtain experimental results has an Intel ®Core™ $^{i3}$ processor M350 (2.27GHz): RAM (4GB): VGA Intel ® HD Graphics, and a 64-bit operating system. Numerous images were subjected to encryption and decryption processes, by both used key generators and Hénon and Lozi maps. Tables 1 shows the full details of examined images.

**Table 1:** Examined Images

| File Name | Examined Image | Image Type | File Size | Image Size |
|---|---|---|---|---|
| Baboon. bmp |  | Gray scale (8 bits/ pixel) | 200kb | 256 x 256 |
| Baboon. bmp |  | Color (24 bits/ pixel) | 200kb | 256 x 256 |
| Pepper. bmp |  | Gray scale (8 bits/ pixel) | 780Kb | 512 x 512 |
| Pepper. bmp |  | Color (24 bits/ pixel) | 780Kb | 512 x 512 |
| Penguin.bmp |  | Gray scale (8 bits/ pixel) | 3400Kb | 1024x1024 |
| Penguin.bmp |  | Color (24 bits/ pixel) | 3400Kb | 1024x1024 |

Table 2 illustrates the level of similarity between original information before encryption, and the extracted information after decryption. The image sizes and files for each sample were kept the same for encryption and decryption.

Table 3 clearly demonstrates that the processing time for encryption and decryption has been influenced directly by the image dimensions. Thus, the smaller sizes image normally required less time for two operation modes. On the other hand the images' colour had a slight impact on the entire process, in spite of the complex nature of colour images which require 24 bit for each pixel if it is compared to a grey one. For larger images the differences between encryption and decryption times are significant. From the above table the difference is about eight seconds for penguin grey and colour images. Hence the proposed solution depended on CTR mode, parallel mode, operation unlike conventional (sequential ) encryption procedures. This will help minimise the required time, which is vital for information security systems especially when applied in a large scale organisations.

When applying the Lozi map the results were extremely similar to those obtained by the Hénon map. Except for penguins, the encryption time for a grey image was 207.78 seconds and required time for decryption was 199.41 seconds, whereas for colour image the encryption and decryption times were 210.27 and 202.885 seconds respectively. So the results using a Lozi map were better than those using a Hénon map for larger images. The proposed solution was repeated using sequential encryption. The required times for the entire operation (encryption and decryption) for all plaintexts were about four times that taken using a CTR operation. That certified a high compatibility of proposed solution for the E-HRM environment.

**Table 2:** Similarity Examination

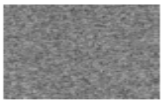
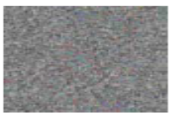
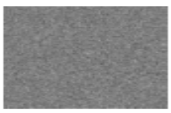
| File Name | Examined Image | Encrypted Image | Encrypted Image |
|---|---|---|---|
| Baboon. bmp 256 x 256 |  |  |  |
| Baboon. bmp 256 x 256 |  |  |  |
| Pepper. bmp 512 x 512 |  |  |  |
| Pepper. bmp 512 x 512 |  |  |  |
| Penguin.bmp 1024x1024 |  |  |  |
| Penguin.bmp 1024x1024 |  |  |  |

**Table 3:** Time of encryption and decryption mode

| File Name | Examined Image | File Size | Image Size | Encryption time ( second ) | Decryption time ( second ) |
|---|---|---|---|---|---|
| Baboon. bmp | Gray scale (8 bits/ pixel) | 200kb | 256 x 256 | 0.866 | 0.848 |
| Baboon. bmp | Color (24 bits/ pixel) | 200kb | 256 x 256 | 0.953 | 0.924 |
| Pepper. bmp | Gray scale (8 bits/ pixel) | 780Kb | 512 x 512 | 10.891 | 10.788 |
| Pepper. bmp | Color (24 bits/ pixel) | 780Kb | 512 x 512 | 10.876 | 10.739 |
| Penguin.bmp | Gray scale (8 bits/ pixel) | 3400Kb | 1024x1024 | 213.35 | 205.81 |
| Penguin.bmp | Color (24 bits/ pixel) | 3400Kb | 1024x1024 | 218.125 | 211.5175 |

## Conclusion

The EHRM is one large scale information system. Thus, sequential or classical encryption is not an appropriate solution for security challenges, especially with truly huge volumes of data used online by EHRM. So in this work the proposed solution was based on cipher mode operation (CTR): to save more time via parallel operation, as well as a high level of complexity which was submitted by using random discrete functions Hénon or Lozi maps. The time required for encryption and decryption was influenced directly by the size of the plaintext, however a significant difference between two conditions is considerable with larger size plaintext (image). Using a Lozi map saved more time with a large plaintext, so the nature of chaotic function affected the performance of the proposed solution. Minimising time reduced the level of threats which face confidential information used by E-HRM.

## REFERENCES

Alpar, O. (2014). Analysis of a new simple one dimensional chaotic map. Nonlinear Dynamics, 78(2): 771-778.

Bissola, R. &Imperatori, B. (2014). The unexpected side of relational e-HRM: Developing trust in the HR department. Employee Relations, 36(4): 376-397.

Bondarouk, T., Harms, R. & Lepak, D. (2017). Does e-HRM lead to better HRM service?. The International Journal of Human Resource Management, 28(9): 1332-1362.

Fay, R. (2016). Introducing the counter mode of operation to compressed sensing based encryption. Information Processing Letters, 116(4): 279-283.

Hashim, M. M., MohdShafryMohd, R., FadilAbassJohi, M.S. T. and Hassan, S. H. (2018). Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. International Journal of Engineering & Technology, 7(4): 3505-3514.

Jain, A. & Goyal, A. (2014). E-Recruitment & E-Human Resource Management Challenges in the Flat World: A Case Study of Indian Banking Industry (With Special Reference to ICICI Bank, Jaipur). International Journal of Scientific and Research Publications, 4(1): 1-8.

Jensen-Eriksen, K. (2016). The role of HR analytics in creating data-driven HRM: Textual network analysis of online blogs of HR professionals.

Khan, M. & Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S 8 symmetric group. Neural Computing and Applications, 25(7-8): 1717-1722.

Kim, P. S. (2016). Innovating training and development in government: The case of South Korea. Sharpening the Sword of State, 125.

Kulkarni, S. R. (2014). Human capital enhancement through e-HRM. IBMRD's Journal of Management & Research, 3(1): 59-74.

Mahdi, M.H., Ali, A.W.A., MohdShafryMohd, R, Mustafa, S. T., HiyamNadhim, K. and Sameer, A.S.L. (2019). Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. In IOP Conference Series: Materials Science and Engineering, 518(5): 052002. IOP Publishing.

Pramanik, S., Singh, R. P. and Ramkrishna, G. (2019). A new encrypted method in image steganography. Indonesian Journal of Electrical Engineering and Computer Science, 14(3): 1412-1419.

Strohmeier, D. E. P. A. P. S. (2014). HRM in the digital age–digital changes and challenges of the HR profession. Employee Relations, 36(4).

Strohmeier, S. & Kabst, R. (2014). Configurations of e-HRM–an empirical exploration. Employee Relations, 36(4): 333-353.

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M. &Alzuabidi, H. M. (2019). May). Combination of Steganography and Cryptography: A short Survey. In IOP Conference Series: Materials Science and Engineering, 518(5): 052003. IOP Publishing .

Xing, Y., Liu, Y., Tarba, S. Y. & Cooper, C. L. (2016). Intercultural influences on managing African employees of Chinese firms in Africa: Chinese managers' HRM practices. International Business Review, 25(1): 28-41.

Zibarras, L. D. & Coan, P. (2015). HRM practices used to promote pro-environmental behavior: a UK survey. The International Journal of Human Resource Management, 26(16): 2121-2142.