SECURING ELECTRONIC HUMAN MANAGEMENT SYSTEM USING COMPATIBLE INFORMATION SECURITY

Muzahim Ryadh Hamdoon, Northern Technical University
Niebal Younis Mohammed, Northern Technical University
Anwar Hadi Aldabbagh, Northern Technical University

ABSTRACT

This work is aimed at studying and describing the compatibility of information security system (ISS) involved in electronic human resources management (e-HMS) which is an aspect of the internet platform that deals with huge volume of private data, such as employees' personal information, important work documents, financial details, as well as technical specifications of specialized products. The solution projected in this study was executed by considering the essential assumption that the private information cannot be altered, and the employees are not allowed to alter the information; hence, this information is handled as images in this study. Another important assumption is the huge amount of e-HMS data that cannot be handled using the traditional/sequential encryption mechanism; such data must first be partitioned into blocks. Hence, in this study, counter mode operation was used to address this issue to save time via parallel operation quality. The generation of the security keys was done using Hénon & Lozi maps; the model proposed in this study ensures a good level of security against cyberattacks like brute force (BF) attack and frequency attack.

Keywords: Vital Information**,** Cyber-attack**,** Hénon and Lozi Maps, Encryption and Security Key Generators.

INTRODUCTION

Management systems play a significant role in any organizational development. As such, Human Management System (HMS) is a vital aspect of the whole management framework and has often been considered in performance evaluation of large-scale organization (Xing, 2016; Zibarras & Coan, 2015). With the advancements in Information Technology (IT) that covers various data forms, it has become important to utilize current technologies for the development of new management systems based on websites. This will require switching from the normal way of HMS to the electronic version of HMS (e-HMS) as this new platform provides good reliability for manager-employee communication by considering the huge data volume (exceeds GB). So, this higher level of compatibility demands that such data be handled in a way that ensures high performance of everyone involved in the management system (Jensen-Eriksen, 2016).

e-HMS is mainly aimed at achieving this high level of compatibility by depending on IT for improving human resources in terms of sharing their private data. The basic aim here is to improve the organizational performance and save cost and time. Therefore, e-HMS has received much attention in different organizations/fields, especially in organizations where the high number of people, systems, time and cost are the major constraints (Bissola & Imperatori, 2014).

e-HMS CLASSIFICATION

The conventional e-HMS can be fundamentally grouped into three groups based on the users aims as follows:

a) Operational e-HMS: The focus here is to utilize technology in all the administrative duties, such as employee payroll & personal information. With operational e-HMS, employees can keep their updated personal data via their organizational websites.
b) Relational e-HMS: This type of e-HMS helps employees to improve their relationship via IT in numerous activities such as online training & discussions, and opinion trading.
c) Transformational e-HMS: Being that several organizations strive to achieve both short and long terms targets, this form of management provides opportunity for the management systems to improve the qualifications of their employees via web-based tools (Strohmeier & Kabst, 2014).

Challenges of Migrating From Normal HMS TO e-HMS

As earlier mentioned, e-HMS is the basic framework in any organization; however, there are certain challenges faced when considering a switch from the normal HRM to the IT-based HRM (e-HMS) and such challenges ought to be carefully considered prior to the adoption of e-HMS as a management style. Among these challenges are the evaluation of the employees and their technical competence in human resource (HR), work process computerization, new service delivery model implementation, reorganization of the HR structure, assignment of new criteria for HR constraints, as well as implementation of HR technology support (Strohmeier, 2014).

Employees are the most vital components of any organization, hence, their attitude towards e-HMS demands investigation as it will contribute to the long-term development and success of the organization and the management system. Here, the departmental heads in an organization have a significant role to play in getting their employees ready for the implementation of the new management system (e-HMS). This implies that the head of departments and organizational heads have a big role to play in breaking the barriers towards implementation of e-HMS. It is natural that people face challenges at the initial stage of any activity; however, their incentives normally increase with continual encouragement as they encounter new situations Bondarouk, et al., 2017)

The Challenges of e-HMS and Security

With e-HMS being an aspect of the IT components of any organization, it is absolutely prone to certain security issues. A huge volume of personal information might be the target of cyberattacks, hence, it is necessary to limit unauthorized access to such information so that they will not be illegally revealed or altered. Achieving a high level of information security in any organization is a tedious task as most security frameworks requires adequate level of license to offer a high level of security (Kulkarni, 2014).

The efficiency of any security system is dependent on: (i) ability to identify confidential information, (ii) ability to detect the expected threats, and (iii) assigning the weakest points in the security system, and (iv) selecting the appropriate solutions and persistent monitoring to evaluate the deployed security system. In the information domain, achieving security requires specific measures, such as the use of password, firewall, legal liability, encryption, antivirus software, and security knowledge. These measures are needed because of the possibility of different types of information security threats. Software attacks are currently considered the commonest and most risky form of threat; this is in addition to other threats such as identity and intellectual property theft. Globally, software attacks are launched as viruses and Trojan horses (Jain, & Goyal, 2014) while identity and intellectual property theft are focused on stealing users' personal information for personal gains. The advancements in communication systems, as well as the increase in the number of internet applications have increased the chances of attacks on users` information; as such, governments and organizations are committing much effort and resources on the security of information systems (Mahdi, et al. 2010).

Both commercial and financial organizations consider information security important for their survival in their competitive environment. The security of employees, customers, and investors information, as well as the quality of products are necessary for achieving long-term goals. Being that e-HMS covers both offline and online information, it is necessary to ensure a good level of coordination among the service providers and the information system managers. Integration of e-HMS as an aspect of organizational management system & ISS requires the full definition of organizational information submitted to an information security system by a management system to enable continuous assessment of the security measures in terms of performance. Figure 1 presents a summary of the proposed system.

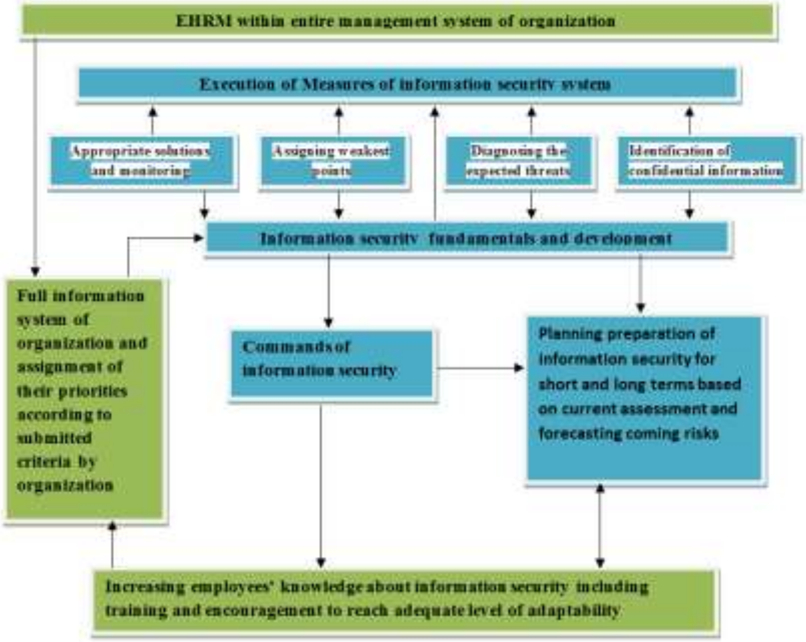
EHRM within entire management system of organization
Execution of Measures of information security system
Appropriate solutions and monitoring
Assigning weakest points
Diagnosing the expected threats
Identification of confidential information
Information security fundamentals and development
Full information system of organization and assignment of their priorities according to submitted criteria by organization
Commands of information security
Planning preparation of information security for short and long terms based on current assessment and forecasting coming risks
Increasing employees' knowledge about information security including training and encouragement to reach adequate level of adaptability

FIGURE 1
INTEGRATION BETWEEN EHRM AND INFORMATION SECURITY SYSTEM

PROBLEM DEFINITION AND THE PROPOSED SOLUTION

Introduction

Globally, different types of organizations generate huge volumes of data in excess of Gigabytes and Terabytes. Hence, different types of data (text and images) are normally exchanged either within an organization or with other organizations. The exchange of such huge data volume is a complicated task that is associated with several complexities. Hence, such complex situations are addressed using information security system (ISS) as such issues demand a high security level. One of the factors considered when building a good ISS is the quality of the security measures employed. In communication systems, encryption is the commonly applied security measure; an encryption framework can be described as a process of encoding important information in a manner that it can only be accessed by an authorized party and unauthorized access by any third party.

Plaintext is information that has been encrypted using any of the encryption algorithms (ciphers). Ciphers are used to generate the ciphertext by the sender while the receiver decrypts the ciphertext to extract the encrypted information. During the encryption process, the security goals are achieved using a security key that is generated using a mathematical function (such as pseudo-random). The pseudo-random generator is a commonly used key generator in security applications. There are two classes of security keys based on their application - symmetric and asymmetric keys. Regarding symmetric key, the encryption and decryption processes are performed using the same key, but for asymmetric key, the security key is only known to the person performing the encryption while the receiver can only read the information.

This study considered two assumptions to achieve a reasonable level of information security in an organization; the first assumption considers the confidentiality of organizational information, including user's personal information, financial documents, etc which are believed to be unalterable. Thus, this class of information are handled as images to guarantee minimum security and robustness against attacks like frequency analyses of the cipher text in which letters are counted to check for the presence of confidential information transmitted as text. The next problem is the huge volume of data that cannot be handled using the conventional encryption approaches. Thus, block cipher modes which breaks huge data into fragments/blocks are required to efficiently handle such big data volumes. Encryption and decryption processes that depend on fixed-length set of bits called block can be done using block ciphers. The operation mode illustrates how a cipher block technique can be implemented to ensure secure data transmission through a block. Generally, the operation mode consists of the initialization vector (IV) which is an exclusive binary chain that is important for any encryption process. The IV may be random but must be non-duplicating (Pramanik, et al., 2019; Fay, 2016).

The IV is used to ensure the generation of dissimilar ciphertexts even when encrypting the same plaintext several times with the same key. Block ciphers can operate on different block sizes; however, the block size normally remains unchanged during the transition. Block cipher modes run on entire blocks and demands the padding of the last part of the data to a complete block (if it is minor) before proceeding to the present block size. Padding simply means the addition of more data to the encrypted confidential information (either to the beginning, middle, or end). Different cipher operation modes have certain drawbacks; however, the commonest mode is Cipher Block Chaining (CBC). In this work, CBC was not used owing to its sequential mode of operation wherein the encrypted information must be padded to several cipher block sizes.

In this research, the Counter Mode operation (CTR) was employed; the CTR saves more time in information handling because it has random access quality unlike CBC. CTR mode is more suitable for meeting the demands of parallel operation compare to the processor and does not experience short-cycle issues. The IV is a counter under this model and the length of the plaintext and counter must be equal before performing the encryption process. CTR works by using the security key (K) to encrypt the value of counter before performing XOR operation on the plaintext (P) to generate the ciphertext (C); at the reception side, the ciphertext (C) will be XORed to obtain the plaintext (P). In this work, two chaotic discrete functions were used to generate the security keys in order to achieve a good level of complexity that will reduce the possibility of an attacker breaching the security protocol of the proposed security solution.

Chaotic discrete functions are highly sensitive to minor changes in the initial condition, meaning that their output can be easily changed due to simple changes. This feature of chaotic systems makes them applicable in several natural and artificial systems across different disciplines, including economics and engineering fields. In this work, Hénon and Lozi maps were used as chaotic discrete functions to generate the keys.

Mathematical Behavior of Used Key Generators

In 1979, the mathematical model of Hénon Map was developed as a 2D function. This map, as described in Equation (1), contributed immensely to the mathematical characterization of discrete dynamic systems experienced from the special response. The obvious random behavior of this map is illustrated in Figure 2.

$$X_{n+1} = 1 - aX_n^2 + bY_n \quad \text{.............} (1)$$

$$Y_n = bX_n$$

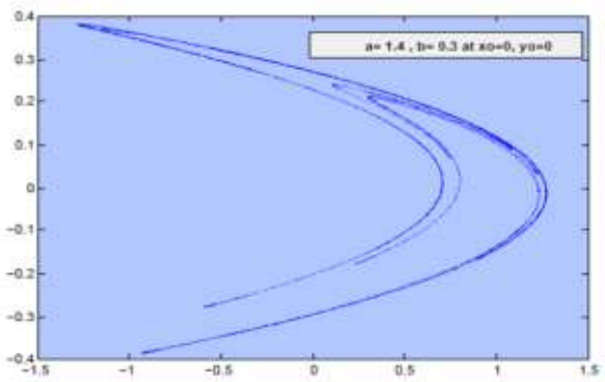

FIGURE 2
CONVENTIONAL HÉNON MAP

Another notable random response of Lozi map as developed in 1978 is also shown in Equation (2). Lozi mathematical model has found application in several fields, such as synchronization theory, control systems, and secure communications. The random behavior of Lozi function is illustrated in Figure (3).

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

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

It should be noted that parameters a & b exerts great influence on the random response shape for both functions (Khan, & Shah, 2014; Taha, 2019).

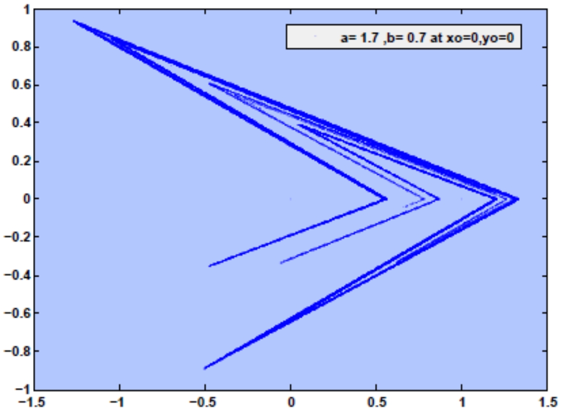

FIGURE 3
CONVENTIONAL LOZI MAP

Procedure of the Proposed Solution

Relying on the assumptions above, images were considered the vital information in this work; the security keys ((random numbers) will be generated using the two key generators. These keys will be transformed into integer within the range of 0 to 255 to ensure the expression of the intensity value of each pixel within the plaintext. The absolute sequence function is needed in the transformation process to avoid negative values as each (Xn) will be multiplied by 1000. The output numbers are normally real values; so, to obtain integer values, the floor function should be used. The entire process is shown in Equation (3):

$$Z_n = \lfloor \| X_n \times 1000 \| \rfloor \text{ .. ……… (3)}$$

Where Z_n is the output integer number and the final value of security key generated by the Hénon or Lozi maps that will be utilized as K in the CTR process. A counter will start from 0 to a maximum value of 255. The proposed security protocol that includes both the encryption and decryption conditions is shown in Figure 4. The quality of parallel operation is obvious as much information can be processed by the users within a specific time. Each organization generates gigabytes of data daily; for instance, some organizations have hundreds of employees that generate more than 100 MB of data daily; hence, the whole data volume for such organization amounts to more than 10 GB and might often be online. Thus, there is a high level of threat as users might lose a significant part or whole of the vital information. Based on the above mapping, the key length and the plaintext length for the proposed study is 8 bits, while there will be 4 encryption & decryption processes (4 blocks will be simultaneously subjected to the process at the same time). The complexity level will be high under practical case while the length of the plaintext block and counter will be 64 bits or 128 bits. Brute force attack will require more time to reveal the secret data while the complexity will increase if there is a significant level of noise in the plaintext shows in Table 1.

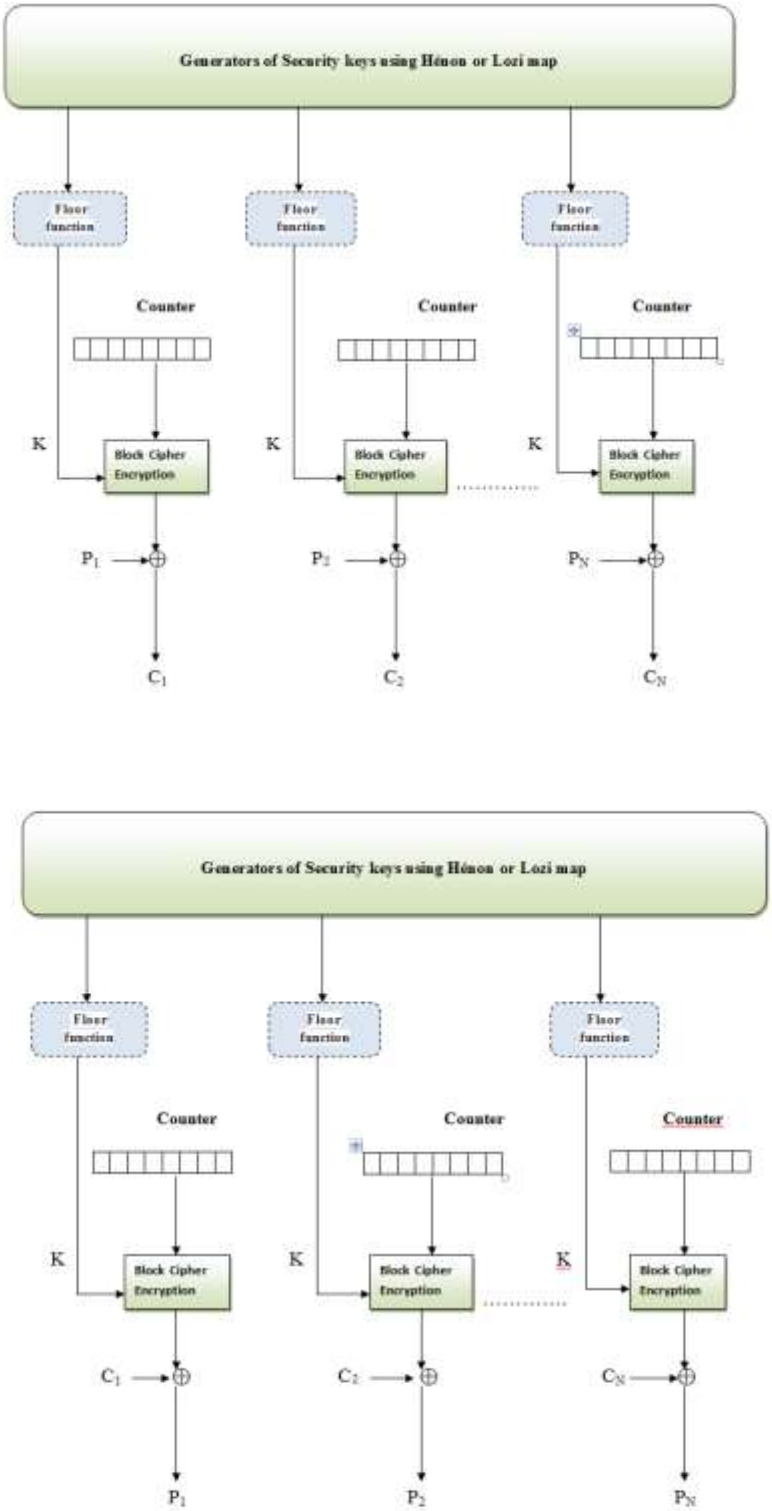

FIGURE 4
PROPOSED ENCRYPTION SYSTEM BASED ON ADVANCED CTR

Table 1
PROPOSED DECRYPTION SYSTEM BASED ON ADVANCED CTR

File Name	Examined Image	Image Type	File Size	Image Size
Baboon		Gray scale image	210kb	256 ×256
Baboon		Color image	210kb	256 × 256
Pepper		Gray scale image	800Kb	512× 512
Pepper		Color image	800Kb	512× 512
Penguin		Gray scale image	3500Kb	1024×1024
Penguin		Color image	3500Kb	1024×1024

RESULTS

The computer used to obtain experimental results has Intel® Core^{TM} i^7processor M350 (4.9 GHz), RAM (8GB), VGA Intel® HD Graphics, 64-bit operating system. A number of images were subjected to the encryption and decryption process by both used key generators Hénon and Lozi maps. Tables 2 dipicts full details of examined images.

The level of similarity between the original data before encryption and the extracted data after decryption is presented in Table 3. During the encryption and decryption processes, the same image sizes and files were maintained. Table 4 showed the obvious influence of the image dimensions on the encryption and decryption process times; thus, smaller-sized images are ideal for two operation modes as they require less processing time. Furthermore, there was a little impact of the image colors on the whole process despite the complexity of the color image which requires 24 bit per pixel compared to the gray image. Significant differences were noted between the encryption and decryption times of the larger sized images. Table 3 showed a difference of about 8 sec between color images and penguin gray images. Thus, the proposed approach relied on CTR mode and parallel operation mode unlike the conventional (sequential) encryption technique. This helps to reduce the required time for both encryption and decryption processes, and it is a significant factor to ISS, especially when deployed on large-scale organizations.

It should be noted that the results achieved with Lozi map were similar to those of Hénon map except for penguin case where the gray image required an encryption time of 207.78 sec and 199.41 sec for decryption while the encryption and decryption times for the color image were 210.27 sec and 202.885 sec, respectively. So, on large-sized images, Lozi map produced better results than Hénon map. The proposed approach was also repeated using sequential encryption processes where the required encryption and decryption times were about four times for all plaintexts compared to CTR operation mode. These findings proved the compatibility of the suggested approach with e-HMS environment.

Table 2
EXAMINED IMAGES

Baboon		Gray scale image	210kb	256 ×256
Baboon		Color image	210kb	256 × 256
Pepper		Gray scale image	800Kb	512× 512
Pepper		Color image	800Kb	512× 512
Penguin		Gray scale image	3500Kb	1024×1024
Penguin		Color image	3500Kb	1024×1024

Table 3
SIMILARITY EXAMINATION IMAGES

File Name	Examined Image	Encrypted Image	Encrypted Image
Baboon 256 ×256			
Baboon 256 ×256			
Pepper 512 ×512			
Pepper 512 ×512			
Penguin 1024 ×1024			
Penguin 1024 ×1024			

Table 4
TIME OF ENCRYPTION AND DECRYPTION MODE

File Name	Examined Image	File Size	Image Size	Encryption Time (Second)	Decryption Time (Second)
Baboon	Gray-Scale Image	210kb	256 ×256	0.866	0.848
Baboon	Color Image	210kb	256 ×256	0.953	0.924
Pepper	Gray-Scale Image	800kb	512 ×512	10.891	10.788
Pepper	Color Image	800kb	512 ×512	10.876	10.739
Penguin	Gray-Scale Image	3500kb	1024 ×1024	213.35	205.81
Penguin	Color Image	3500kb	1024 ×1024	218.125	211.5175

CONCLUSION

Being that e-HMS is among the large-scale information systems, the associated security challenges of e-HMS may not be properly managed using sequential or classical encryption considering the huge data volume used online by e-HMS. Thus, this work proposes CTR-based parallel operation to save more time; the use of random discrete functions (Hénon or Lozi maps) was also proposed to improve the level of complexity. The outcome of this study showed direct influence of the plaintext size on the encryption & decryption times. However, the performance of the two conditions differed considerably with larger sized plaintext. The type of chaotic function utilized also affected the performance of the proposed solution as more time was saved with Lozi map on large sized plaintext. The threats to confidential e-HMS information can be reduced by minimizing the encryption and decryption times.

REFERENCES

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

Bondarouk, T., Harms, R., & Lepak, D. (2017). Does e-HMS 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.

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

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.

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

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

Mahdi, M.H., Ali, A.A., Mohd Shafry, M.R., Mustafa, S.T., Hiyam Nadhim, K., & Sameer, A.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).

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

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

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).

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

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.