Kufa Journal of Engineering
Vol. 16, No. 4, October 2025, P.P. 252-267
Article history: Received 30 November 2024, last revised 23 January 2025, accepted 26 January 2025

EVALUATING THE DIVERSE EFFECTS OF SIGNATURE ENCRYPTION ON MVS SYSTEM PERFORMANCE

Roaya S. Abdalrahman [1], Ali Adnan Wahbi[2] and Abdulrahman I. Siddiq[3]

[1] Mrs. Roaya S. Abdalrahman, Electronic and Control Department, Technical Engineering College Kirkuk, Northern Technical University-Iraq and rouya.abdalrahman@ntu.edu.iq

[2] Mr. Ali A. Wahbi, Electronic and Control Department, Technical Engineering College Kirkuk, Northern Technical University-Iraq and ali.adnan@ntu.edu.iq

[3] Dr. Abdulrahman I. Siddiq, Electronic and Control Department, Technical Engineering College Kirkuk, Northern Technical University-Iraq and draisiddiq@ntu.edu.iq

https://doi.org/10.30572/2018/KJE/160415

ABSTRACT

Recently, image content based information retrieval has been widely used in many applications. A Mobile Visual Search (MVS) system involves capturing an image for the object to be searched for, extracting useful features, constructing object signature and searching local and/or remote databases for a match. This paper investigates the diverse effects of signature encryption on the accuracy, search burden and response time of an MVS system. The aim of this research is to provide a comprehensive understanding of the implications of signature encryption to figure out the design trade-offs that facilitate better MVS performance under given operation hypotheses. An MVS system employing different signature encryption algorithms is simulated with different system parameters. The obtained results show that signature encryption generally adds to system processing time from 5.9 µs to about 22.7 µs in test cases 4 and 6. Moreover, it makes the MVS system more sensitive to imaging and communication link imperfections leading to less capability to correctly identify entries and increased search and transmission loads from 1984 to 8075 requests to access the main database for test cases 3 and 9. These effects depend on the features of the specific encryption algorithm. Therefore, a trade-off between system performance and required security level should be considered to achieve a target performance suitable for the intended application.

KEYWORDS

MVS, Signature encryption, Local database, Network load, Matching.

1. INTRODUCTION

In an era marked by the rapid proliferation of Mobile Visual Search (MVS) Systems, ensuring the security and integrity of visual data has become a paramount concern (Lee et al., 2017). One crucial aspect of safeguarding this information lies in the application of signature encryption, a practice aimed at protecting the authenticity and confidentiality of visual signatures captured by MVS. As MVS technologies continue to evolve and find applications in various domains such as surveillance, transportation, and healthcare, understanding the nuanced impact of signature encryption on system performance measures becomes imperative. Mobile visual search systems, comprising image capture devices and intelligent processing units, are instrumental in extracting valuable information from visual data (Sultan, Nora,2021). The rise in the use of MVS has prompted a parallel emphasis on securing the integrity of the captured data, particularly when it involves sensitive or personally identifiable information. Signature encryption emerges as a key solution, offering a layer of protection against unauthorized access, tampering, or interception of visual signatures within the MVS framework (Al-Asady, Heba et al., 2024). While the adoption of signature encryption in MVS is vital for data security, its implementation may introduce a range of effects on system performance. The term signature encompasses a diverse array of visual patterns, including license plates, facial features, and object recognition cues. Consequently, the encryption methods employed to secure these signatures can exhibit varied impacts on processing speed, accuracy, and other performance metrics within the MVS. This research endeavors to systematically evaluate the diverse effects of signature encryption on MVS system performance. By conducting a comprehensive analysis, we aim to uncover the nuanced trade-offs and challenges associated with implementing signature encryption methods in the context of mobile vision applications. The study seeks to contribute valuable insights that inform the design, implementation, and optimization of secure MVS systems without compromising critical performance aspects. While this study delves into the multifaceted impacts of signature encryption, it is essential to acknowledge the inherent limitations. The scope of this research primarily focuses on a select set of encryption methods and performance metrics, recognizing that the landscape of encryption techniques and MVS applications is vast. Furthermore, the findings are contingent on the specific experimental setup, and variations in real-world scenarios may exist. MVS based systems have become of the most important and widely used systems in many fields, such as identifying products (Girod et al., 2011), shopping (Dagan et al., 2023), electronic libraries (Duan et al., 2014), identifying archaeological sites (Chandrasekhar et al., 2011), and Keyword Search in Real-World Scenes (Pundlik et al., 2019). By using local features and memory-efficient image databases, a low-

latency mobile visual search system may be created, minimizing the need to query a remote server (Chen and Girod, 2014). Many works have studied different aspects of the MVS system to evaluate and enhance its performance. That is, low bit rate wireless transmission has been studied in the context of visual search by sorting local descriptors on a mobile device in (Chen et al., 2011). A new scheme for mobile visual search is proposed by reducing the query image size to achieve low bit rate visualization (Tan et al., 2016). Also, to improve the visual search, an active approach to visual search based on sensory information provided by the camera, is introduced. For the same purpose, a mobile visual recognition scheme has been developed in (Gui et al., 2013). Another way to improve visual search is presented in (Qi et al., 2017) by generating hash-like binary codes with an efficient deep learning system based on. In many real applications, query images are classified into separate quality levels. A quality-aware system for visual search on mobile devices has been created based on a fusion method and query quality in (Peng et al., 2014). However, it has been suggested that matching performance can be improved by integrating image and text features into a mobile visual search system (Tsai et al., 2011). A cluster-based descriptor classification method was applied to the descriptor database. It was found that the proposed method significantly reduces memory consumption while maintaining high matching accuracy (Chen and Koskela, 2011). In addition, a hybrid system was applied to query and match data with the mobile database or the server database to reduce query time (Chen and Girod, 2015). It was pointed out in (Girod et al., 2011) that storing a small-sized image database locally and performing the matching directly on the device can significantly improve the visual search. This idea can be applied to various applications, including cars, smart TV, entertainment and surveillance. The incorporation of security protocols in MVS systems has been considered in applications where the signature involves personal and critical information. However, in this context there are a wide variety of security methods that differ in the achievable security level and computational complexity. The usage of signature encryption/decryption can have both positive and negative effects on the performance of MVS systems, depending on the specific protocols implemented and the overall design. Security protocols may impact the MVS system in terms of network load, search load, and the probability of correct matching:

A. Network Load: This is related to the intensity of information traffic passing through the communication links connecting the distributed system devices. Basically, encryption and secure communication protocols can protect data in transmission but may add a minimal overhead to the network load. Many modern encryption algorithms are designed to be efficient (Yang et al., 2024), and the impact on network performance may be negligible. On the other

hand, if the chosen encryption algorithms are computationally intensive or if the secure communication protocols introduce additional handshake or authentication steps, they could lead to increased latency and higher network utilization (Shen et al., 2019).

B. Search Load: In real applications, the databases to be searched contain a large number of items stored as numerals, plain or coded images. The search load is a critical parameter to determine the response time of MVS systems. In this context, authentication and authorization mechanisms can help control access to the MVS, preventing unauthorized users from initiating searches and reducing unnecessary search loads on the system (Sharma and Kaushik, 2019). But, unfortunately employing strong authentication measures may add processing overhead, impacting the speed of user access. Additionally, if security measures are too restrictive, they might hinder legitimate users, resulting in longer response times for search queries (Ma et al., 2015).

C. Accuracy: The accuracy is related with the capability of the MVS system to correctly identify and classify an object based on its signature. Generally, security measures such as encryption and secure communication, can contribute to the overall system reliability and integrity, ensuring that data is not tampered with during transmission. This enhances the probability of correct matching by reducing the risk of data corruption (Ren et al., 2021). On the other hand, overly complex security measures, if not implemented properly, could introduce errors or delays in data transmission, potentially affecting the accuracy and timeliness of matching algorithms. For instance, if secure communication protocols introduce delays, it might impact the real-time nature of certain MVS applications. Also, an encrypted signature sent to a remote database is exposed to communication channel impairments leading to errors in the decrypted version and hence matching errors.

The available literature on MVS systems has shown the diverse effects of the used signature security scheme on the overall system performance. Then, the careful selection and implementation of security protocols are crucial to balancing security and performance in a specific MVS. That is, a well-designed and properly implemented security framework should enhance the reliability and trustworthiness of the MVS system without significantly compromising its performance. Therefore, this paper aims to evaluate the effects of signature encryption algorithms belonging to different classes, on the performance of an MVS system evaluated under constraints simulating practical operation conditions such as limited local storage, imperfect imaging system (Qasim, Sara et al., 2024) and communication link impairments.

2. SYSTEM MODEL

The MVS system in this paper is developed to serve as car identification system. It provides the facility to identify and retrieve information of a car in response to its image. As shown in Fig.1, the model of the MVS system consists of a central main database and many local databases equipped with a visual system that can capture car image and construct a suitable signature, including car ID number and other features, to be used as the search key in the database.

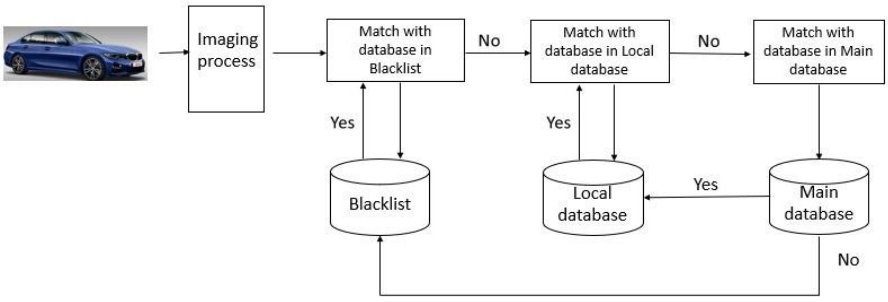

Fig. 1. Block diagram of basic car identification MVS system

The adopted hypothesis assumes that the main database initially holds the necessary information on the registered cars and it is linked with the local databases. In real operation, the system should be able to identify whether a car is registered in the system or not. For registered cars, the car information should be available at the locations of the local databases whenever it is asked for. The system starts operation from an initial state where the local databases are empty. On the arrival of a car at the location of a certain local database, its identification signature is generated and sent to the main database to be searched for, if it matches an item, then the related information is sent back to the local database to be registered and used to activate some action, such as opening a gate. Thereby, the local databases are cumulatively built, reducing the need to bother the main database with repeated queries. In addition, part of the local database storage space is reserved to hold a black list of unrecognized cars. These are the cars that are not registered in the main database. To minimize the search and communication burden on the system, the signature of the car being processed is first searched for in the local black list, if it is found, then it is directly rejected and the system stops. Otherwise, the signature is searched for in that local database. If a match occurred, the suitable action is performed, or else the signature is forwarded to be searched for in the main database. The result should be one of two possibilities; the first is when a match is got, in this case the related information is sent back to the local database to be updated as described before. The second possibility is when no match is achieved, then this car is recognized as an unregistered entry in the system and a signal is fed back to the local database to add this car signature to the black list. However, to maintain the security of the data being stored and exchanged within the system (Xu et al., 2021), a data

encryption protocol is used to protect transmitted data and the contents of the databases from being accessed by unauthorized users. In order to evaluate the effect of utilizing signature encryption on the performance of the MVS system, two well-known standard data encryption techniques has been used namely the Advanced Encryption Standard (AES) and the Rivest, Shamir, and Adleman (RSA). These methods were chosen to exemplify the two primary categories of data encryption: symmetric and asymmetric classes. AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. It is commonly and efficiently used for securing sensitive data like file encryption, disk encryption, and communication protocols, such as the TLS (Transport Layer Security) protocol. RSA, on the other hand, is an asymmetric encryption algorithm that uses a pair of public and private keys. It is commonly used for secure communication, digital signatures, and key exchange. RSA tends to be slower compared to symmetric algorithms like AES because of the mathematical operations involved in key generation and encryption/decryption. However, in practice, the choice between AES and RSA depends on the specific security requirements of the system (Hamza and Kumar, 2020; Chandel et al., 2019).

3. METHODOLOGY

The performance of MVS systems is related to the signature processing, transmission, storage, and consequently the probability of getting correct matching and system response time. That is, the more complex and longer signature processing and/or transmission time lead to slower system response in terms of database search time and data retrieval. The database search time is also affected by the accuracy of the extracted signature, which is in turn affected by the imperfections of the imaging system and transmission links, and most importantly by the computations of the used security algorithm. The signature accuracy has a vital impact on the probability of getting a correct match in the searched database. Then, the performance of the MVS system is mainly characterized by the following metrics:

Response time: the average time required by the system to respond to a request.

Accuracy: the capability of the system to get correct matching at both the main and local databases under the effect of different error sources.

Resource utilization: the increase in main database usage and hence signature encryption/decryption and transmission, due to system imperfections.

In this paper, a software simulation to the MVS system described in section 2 is developed. Its performance is tested and evaluated under different operation conditions, as follows:

To verify the basic principle of operation, a baseline MVS system is developed with no limit

on the local storage, perfect imaging system and perfect channel between the local and main databases.

The AES and RSA signature encryption algorithms are incorporated into the baseline MVS system to evaluate their individual effects.

Then, the system is tested under limited local storage, imperfect imaging and local to main database channel impairments, to simulate practical operation conditions.

In each test case, the main MVS system parameters that can describe the performance are recorded, compared and analyzed. The implemented test cases are summarized in Table 1.

Table 1. MVS system test cases

Test case	Signature encryption	Limited local storage	Perfect imaging system	Perfect local to main channel	Description
1	NO	NO	YES	YES	Perfect baseline MVS system
2	AES	NO	YES	YES	MVS with AES signature encryption
3	RSA	NO	YES	YES	MVS with RSA signature encryption
4	NO	YES	YES	YES	Baseline MVS with limited local storage
5	AES	YES	YES	YES	MVS with AES and limited local storage
6	RSA	YES	YES	YES	MVS with RSA and limited local storage
7	NO	YES	NO	YES	Baseline MVS with limited local storage and imperfect imaging system.
8	AES	YES	NO	YES	MVS with AES, limited local storage and imperfect imaging system.
9	RSA	YES	NO	YES	MVS with RSA, limited local storage and imperfect imaging system.
10	NO	YES	YES	NO	Baseline MVS with limited local storage and imperfect local-to-main link.
11	AES	YES	YES	NO	MVS with AES, limited local storage and imperfect local-to-main link.
12	RSA	YES	YES	NO	MVS with RSA, limited local storage and imperfect local-to-main link.

The MVS system described in section 2 is simulated in MATLAB. The main database is loaded with the data of 1000 registered cars. The records contain the identification number, ID, and the related car information. A test list of 10000 cars is randomly generated that is used to initiate the requests for testing the performance of the MVS system. The test list involves cars that are registered in the main database and others not registered, with random repetitions to simulate the request to identify cars that appear at the location of the local database more than once. The same test list is used with the different test scenarios in this work to evaluate and compare the performance of the system under different operation conditions. As described in section 2, the main database is un-updateable, whereas the local database and the black list are initially empty and they are cumulatively built up.

However, the MVS system takes different periods of time to respond to different car situations, such as registered, unregistered, repeated and not repeated. The average system response, T_{av}, depends on the number of times each database is searched and the time required by each search.

It is defined as:

$$T_{av} = (S_M t_M + S_L t_L + S_B t_B) /N \quad (1)$$

Where

S_M, S_L and S_B are the number of times the main, local and black list databases are searched, respectively.

t_B is the average time elapsed to search the black list. The black list database is initially empty, then the increases as it builds up.

t_L is the average time spent when the local database is searched. This includes the search time in the black list plus the search time in the local database. This is because, as described in the system model section, a new request is first checked in the black list and if it does not match any of its entries, then it is searched for in the local database.

t_M is the time required for an item to be searched for in the main database. This occurs after the search in the local and black list databases fails to get a match. Generally, this time also includes the signature transmission, encryption and decryption, and information reception times.

N is the total number of items in the test list, which is set to 10000 in this simulation.

It worth noting that the number of matches in the main database, M_M, is equal to the final size of the local database, L_L, since the latter represents the number of items found in the main database and sent back and stored in the local database to avoid repeating the same request from the main database when the same cars appear again in the future. In addition to L_L, the main database is searched times when unregistered items enter the system. Then, the total number of accessing the main database to search for an item, S_M, is equal to $(L_L + L_B)$, with each access requiring t_M. Moreover, S_L, is equal to $(N - M_B)$ since excluding the cars that find matches in the black list, all of the rest cars should be searched for in the local database. Whereas, S_B is equal to the number of cars in the test list (10000) since on the arrival of each car it is immediately searched for in the black list. Then, T_{av}, can be rewritten as:

$$T_{av} = ((L_L + L_B)t_M + (N - M_B)t_L + N t_B) /N \quad (2)$$

In summary, for the test cars, there are four possibilities in this system, in Table 2 as follows

Table 2. Summary of operation in test cases 1 through 6

Appearance in the test list	Registered	Not registered
Once	Find M_M matches in the main database. Then, making the final length of the local database $L_L = M_M$.	Search the main database L_B times without getting a match. Then, making the final length of the black list database $S_L - M_M - M_L$.
More than once	Find M_L matches in the local database.	Find M_B matches in the black list database.

Therefore, if the signatures have been correctly recognized and classified by the MVS system, then the numbers of registered, N_{reg}, and unregistered, N_{unreg}, cars in the test list are given by:

$$N_{reg} = M_M + M_L \quad (3)$$

$$N_{unreg} = S_L - M_M - M_L + M_B \quad (4)$$

The sum $(S_L + M_B)$ is equal to N. The schematic diagram shown in Fig. 2 describes the operation of the MVS system and the relation between its parameters.

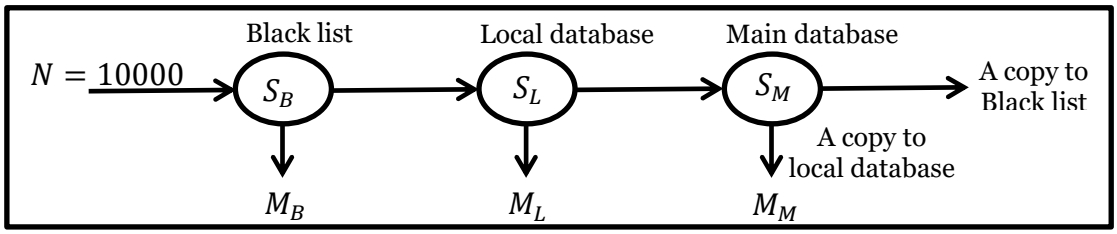

Fig. 2. MVS system parameters

4. SIMULATION RESULTS AND DISCUSSION

First of all, as a reference case, the baseline MVS system is simulated with ideal parameter values. It is assumed that the imaging system can perfectly extract the car ID number to construct the signature. Also, a perfect communication channel and no signature encryption between the local and main databases are assumed, with an unlimited storage size at the local database. The obtained results are shown in Table 3, test case 1, for the number of matches in the main, M_M, local, M_L, and black list, M_B, databases and the final storage memory length at the local, L_L, and black list, L_B, databases in terms of the number of stored records. Moreover, as a measure for the speed of the system, the average response time, T_{av}, of the MVS system for the 10000 requests under the assumed system setup is measured and recorded.

Table 3. Results of test cases 1 through 6

Test case	T_{av} (μs)	M_M	M_L	M_B	L_L	L_B	S_M	S_L
1	2.5902							
2	5.1694	994	3998	4018	994	990	1984	5982
3	6.7566							
4	5.9149							
5	16.35	4005	987	986	200	200	8027	9014
6	22.7716							

Encryption is used to maintain the security of the traffic sent and received from the main database, namely the signature and the retrieved information. The AES and the RSA are used to represent the two main data encryption classes of symmetric and asymmetric algorithms. For the AES, a 128-bit key and the Galois/Counter Mode (GCM) block cipher mode are used. For the RSA, the used public and private keys are (17,77) and (53,77), respectively. For both schemes, it is assumed that the keys are available where they are required. The results shown in Table 3, test cases 2 and 3, show the direct effect on the average system response time. The

RSA algorithm is more computationally intensive than the AES, resulting in longer T_{av}. The use of data encryption has no effect on the system performance in terms of the number of matches and searches in the databases. That is the MVS system still has the ability to correctly identify and classify each car ID and signature. This is because the used encryption algorithms are lossless and also due to the ideal assumptions made for the baseline system. However, in practice, this is not the case. Therefore, the system is tested with different settings simulating practical conditions. The effect of limited local and black list memory size, imperfect signature generation and noisy channel between local and main databases, are evaluated individually and collectively. Table 3 also shows the results of test cases 4, 5 and 6 for the often practical situation of limited system resources, namely the limited memory space in the local equipment. The capacity of the local and black list is taken to be 200 records each. It can be observed from the obtained results that the search load has been skewed towards the main database. That is the first appearing 200 registered and 200 unregistered cares are recorded in to the local and black list databases, respectively. Any similar cars are no longer recordable in these databases and they should be searched for in the main database whenever they appear. It worth noting that ability of the MVS system in correctly recognizing and classifying the signatures has not been affected by the limited local storage. However, the resulted increase in the search burden in the main database and the associated increase in communication load, have consequently increased the system average response time, T_{av}. These results show the direct trade-off between the availability of system resources, local storage in this case, with MVS system performance metrics such as database search load and T_{av}. The choice of the signature encryption algorithm also makes a difference. That is, more access to the main database leads to more signature encryption and in turn longer T_{av}. Another factor that can affect the performance of the MVS system is the efficiency of the imaging subsystem. The captured car images are corrupted with Additive White Gaussian Noise (AWGN) with different Signal-to-Noise Ratio (SNR) values to simulate the practical situations of weak lighting and low clarity conditions that affect the accuracy of the ID recognition algorithm. The results are shown in Table 4 for the test cases 7, 8 and 9. The very clear observation is that the MVS system has started to make incorrect decisions on a number of items of the test list. That is, when the results of test case 7 are compared with that of test case 4 in Table 3, it can be noted that the system fails to correctly recognize some noisy signatures, leading to wrong classification and treatment, which is clear from the values of M_L and M_B. Moreover, noisy signatures together with the constraint of limited local database storage increase the search burden in the local and main databases resulting in slower system response. Although these effects get less as SNR increases making

the performance metrics closer to test case 4, but the MVS system continues to have deviations. Similarly, the same comments hold for the results of test cases 8 and 9, shown in Table 4.

Table 4. Test cases 7, 8 and 9

SNR (dB)	Test case 7						Test case 8						Test case 9					
	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L
1	6.45	2390	9574	8992	426	582	19.06	1252	302	209	9489	9489	27.53	508	106	73	9821	9927
5	6.28	2938	9429	8678	571	751	18.29	2205	565	363	9072	9072	27.18	852	173	139	9688	9861
10	6.15	3378	9291	8443	709	848	17.56	3036	751	574	8675	8675	25.82	2058	484	340	9176	9660
20	6.01	3823	9117	8195	883	922	16.70	3684	966	821	8213	8213	24.11	3200	828	645	8527	9355
30	5.97	3976	9061	8126	939	935	16.56	3916	938	920	8142	8142	23.18	3742	948	874	8178	9126
40	5.91	3974	9010	8013	990	997	16.27	3944	1013	1003	7984	7984	23.04	3976	919	951	8130	9049
50	5.93	4010	9034	8059	966	975	16.34	3992	989	992	8019	8019	22.88	3990	970	964	8066	9036
60	5.91	3991	9024	8024	976	1000	16.45	4043	946	973	8081	8081	22.90	4050	929	996	8075	9004

It should be noted that the degradation in MVS system performance characterized by longer average response time, is indirectly caused by signature encryption. That is when noisy signatures cause an increased demand to access the main database, then by definition increase the number of times of signature encryption/decryption and hence T_{av}. Finally, the effect of imperfect communication channel used to convey encrypted signatures is evaluated. Without loss of generality, an AWGN channel between the local and main databases is assumed. The encrypted signatures are corrupted with noise while they pass the channel towards the main database when no match is got in the black list and the local database. As in practice, the communication system employs channel coding for error detection and correction. A (7,4) Low Density Parity Check (LDPC) code is incorporated in the simulated MVS system. The results of test cases 10, 11 and 12 are shown in Table 5. As compared with test cases 4, 5 and 6 in Table 3, it can be stated that the channel noise has a limited effect on the accuracy of signature classification. Thanks to the used LDPC coding and its role in getting rid of most of channel errors. Therefore, the channel noise has a limited effect on the average system response time. Then, in the case of noisy channel, the dominant factor on T_{av} is the computations involved in the adopted signature encryption method. Generally, high security levels are achieved by using relatively computationally complex encryption algorithms.

Table 5. Test cases 10, 11 and 12

SNR (dB)	Test case 10						Test case 11						Test case 12					
	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L	T_{av} (µs)	M_M	M_L	M_B	S_M	S_L
1	5.98	3662	850	989	8161	9011	16.76	2181	756	989	8255	9011	23.42	976	726	999	8275	9001
5	5.97	4331	868	1000	8132	9000	16.66	3456	828	976	8196	9024	23.29	1552	774	998	8228	9002
10	5.97	4423	878	978	8144	9022	16.49	4390	911	985	8104	9015	23.30	3212	796	975	8229	9025
20	5.95	4065	931	982	8087	9018	16.56	4092	877	981	8142	9019	22.92	4402	892	1021	8087	8979
30	5.99	4140	841	985	8174	9015	16.59	4116	865	976	8159	9024	23.10	4140	879	970	8151	9030
40	5.95	4071	919	984	8097	9016	16.54	4111	876	990	8134	9010	23.12	4142	860	980	8160	9020
50	5.96	4085	906	986	8108	9014	16.51	4092	901	986	8113	9014	22.96	4077	913	988	8099	9012
60	5.94	4051	938	986	8076	9014	16.39	4024	967	986	8047	9014	22.87	4035	950	986	8064	9014

This imposes a trade-off between the required level of signature security with the complexity of the encryption algorithm and hence T_{av}. On the other hand, imperfect imaging can cause more significant performance degradation, because the system deals with a distorted version of the signature. However, a common feature between the effects of imperfect imaging and main to local channel is that the MVS system can no longer obey the Eqs. (3) and (4). This is because the inaccuracy in the processed signatures leading to an extra search and transmission loads and hence longer average system response time.

5. CONCLUSIONS

In this paper, the diverse effects of signature encryption on the performance of MVS system have been evaluated. The obtained results show that in the case of perfect system parameters such as the imaging system, transmission and unlimited local storage size, and then signature encryption does not affect the ability of the system to correctly identify and classify the cars. The only effect is the elongation of the system response time from 2.5902 µs to about 2.5 µs and 6.8 µs. This directly depends on the computational complexity of the used encryption algorithm. This result shows a trade-off between the required level of security and MVS response time. Next, the system performance is highly affected by the limitation in the local database storage. This limits the number of cars that can be stored in the local database and then increases access and search loads on the main database. For the tested system the search requests in the main database has increased from 994 to 4005 when the size of the local database is limited to 200 items. This in turn demands more signature transmission, encryption/decryption, and consequently resulting in longer system response time of up to 22.77 µs as in test case 6. Therefore, for limited local storage it is better to employ simpler encryption algorithms to maintain reasonable system response time. Or else, if the security of the signatures is a critical issue, then there should be an enough local storage to accommodate the largest possible number of records to avoid increasing the demand to access and search the main database. Moreover, inaccurate signature construction due to imperfections in the components of the imaging system can significantly degrade the MVS system performance. The effect is two folds, firstly the MVS system is no longer able to correctly identify and classify the cars. That is some distorted signatures of registered cars may be considered as unregistered and vice versa. Secondly, the noisy signatures together with limited local storage can impose an extra load on the main database to be accessed and searched, from 1984 to 8075 requests to access the main database for test cases 3 and 9. This results in longer system response time, as in test case 9 where Tav has increased from 22.9 µs to 27.5 µs. Therefore, it

can be concluded that the use of accurate imaging, feature extraction equipment and maintaining suitable lighting conditions have a significant effect on the performance of the MVS system in terms of correct operation and response time. Finally, the obtained results for the effect of imperfect communication channel that conveys encrypted signature between the local and main databases is much less than the effect of imperfect imaging. This is due to the error control channel coding and the detection algorithms that are capable of correcting most of the errors in the received encrypted signatures. However, the nature of the employed encryption algorithm has a significant role in determining the exact effects. That is, more computationally complex encryption algorithms can maintain high security level to the signatures being transferred within the system, but this advantage is at the expense of longer processing time and slower system response, and most importantly more sensitivity to system imperfections. The choice of the specific signature encryption algorithm should consider the trade-off between the required quality of service defined by MVS system performance metrics and the available resources such as the local storage size, suitable imaging and transmission system. Therefore, this research figures out many interesting future research gaps and perspectives. Specific standard or modified encryption algorithms could be tested. Having random parameters in the system such as the imaging noise and random entries, make it useful to explore their effects by conducting a more in depth statistical analysis to the obtained results. Also, to evaluate the system under specific realistic application conditions, the practical implementation and the effect of the associated hardware and software parameters, imaging conditions, etc, is a wide area for future research.

6. REFERENCES

Abdul-Jaleel Al-Asady, Heba, et al. “AN IMAGE ENCRYPTION METHOD BASED ON LOGISTICAL CHAOTIC MAPS TO ENCRYPT COMMUNICATION DATA”. Kufa Journal of Engineering, vol. 15, no. 4, Nov. 2024, pp. 55-64, https://doi.org/10.30572/2018/KJE/150405.

Chandel, A., Aggarwal, A., Mittal, A., and Choudhury, T., 2019. Comparative analysis of AES & RSA cryptographic techniques. 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, pp. 410–414. Available at: https://doi.org/10.1109/ICCIKE47802.2019.9004338 [Accessed 20 Nov. 2024].

Chandrasekhar, V.R., et al., 2011. The Stanford mobile visual search data set. Proceedings of the Second Annual ACM Conference on Multimedia Systems, pp. 117–122..

Chen, D.M. and Girod, B., 2014. Memory-efficient image databases for mobile visual search. IEEE MultiMedia, 21(1), pp. 14–23. Available at: https://doi.org/10.1109/MMUL.2013.46 [Accessed 20 Nov. 2024].

Chen, D.M., and Girod, B., 2015. A hybrid mobile visual search system with compact global signatures. IEEE Transactions on Multimedia, 17(7), pp. 1019–1030. Available at: https://doi.org/10.1109/TMM.2015.2427744 [Accessed 20 Nov. 2024].

Chen, J., Duan, L.-Y., Ji, R., Yao, H. and Gao, W., 2011. Sorting local descriptors for low-bit rate mobile visual search. 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, Czech Republic, pp. 1029–1032. Available at: https://doi.org/10.1109/ICASSP.2011.5946582 [Accessed 20 Nov. 2024].

Chen, X. and Koskela, M., 2011. Mobile visual search from dynamic image databases. Image Analysis: 17th Scandinavian Conference, SCIA 2011, Ystad, Sweden, May 2011, Proceedings 17. Springer, pp. 196–205.

Dagan, J.A., Guy, I. and Novgorodov, S., 2023. Shop by image: Characterizing visual search in e-commerce. Information Retrieval Journal, 26(1), p. 2.

Duan, L.-Y., Ji, R., Chen, Z., Huang, T. and Gao, W., 2014. Towards mobile document image retrieval for digital library. IEEE Transactions on Multimedia, 16(2), pp. 346–359. Available at: https://doi.org/10.1109/TMM.2013.2293063 [Accessed 20 Nov. 2024].

Girod, B., Chandrasekhar, V., Grzeszczuk, R., and Reznik, Y.A., 2011. Mobile visual search: architectures, technologies, and the emerging MPEG standard. IEEE MultiMedia, 18(3), pp. 86–94. Available at: https://doi.org/10.1109/MMUL.2011.48 [Accessed 20 Nov. 2024].

Girod, R.B., et al., 2011. Mobile visual search. IEEE Signal Processing Magazine, 28(4), pp. 61–76. Available at: https://doi.org/10.1109/MSP.2011.940881 [Accessed 20 Nov. 2024].

Gui, Z., Wang, Y., Liu, Y., and Chen, J., 2013. Mobile visual recognition on smartphones. Journal of Sensors, Article ID 2013. Available at: https://doi.org/10.1155/2013/2013 [Accessed 20 Nov. 2024].

Hamza, A., and Kumar, B., 2020. A review paper on DES, AES, RSA encryption standards. 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, pp. 333–338. Available at: https://doi.org/10.1109/SMART50582.2020.9336800 [Accessed 20 Nov. 2024].

Lee, E., et al., 2017. Development of gate security system based on mash-up framework. 2017 Third Asian Conference on Defence Technology (ACDT), Phuket, Thailand, pp. 70–74. Available at: https://doi.org/10.1109/ACDT.2017.7886160 [Accessed 20 Nov. 2024].

Ma, R., Li, J., Guan, H., Xia, M., and Liu, X., 2015. EnDAS: Efficient encrypted data search as a mobile cloud service. IEEE Transactions on Emerging Topics in Computing, 3(3), pp. 372–383. Available at: https://doi.org/10.1109/TETC.2015.2445101 [Accessed 20 Nov. 2024].

Peng, P., Li, J., and Li, Z.-N., 2014. Quality-aware mobile visual search. Procedia-Social and Behavioral Sciences, 147, pp. 383–389.

Pundlik, S., Singh, A., Baghel, G., Baliutaviciute, V. and Luo, G., 2019. A mobile application for keyword search in real-world scenes. IEEE Journal of Translational Engineering in Health and Medicine, 7, pp. 1–10. Available at: https://doi.org/10.1109/JTEHM.2019.2935451 [Accessed 20 Nov. 2024].

Qi, H., Liu, W., and Liu, L., 2017. An efficient deep learning hashing neural network for mobile visual search. 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, Canada, pp. 701–704. Available at: https://doi.org/10.1109/GlobalSIP.2017.8309050 [Accessed 20 Nov. 2024].

R. Qasim, Sara, et al. “A NEW NESTED HYBRID DWT-HD-SVD WATERMARKING SCHEME FOR DIGITAL IMAGES”. Kufa Journal of Engineering, vol. 15, no. 4, Nov. 2024, pp. 65-82, https://doi.org/10.30572/2018/KJE/150406.

Ren, X., et al., 2021. Matching algorithms: fundamentals, applications and challenges. IEEE Transactions on Emerging Topics in Computational Intelligence, 5(3), pp. 332–350. Available at: https://doi.org/10.1109/TETCI.2021.3067655 [Accessed 20 Nov. 2024].

Sharma, S. and Kaushik, B., 2019. A survey on internet of vehicles: applications, security issues & solutions. Vehicular Communications, 20, Art. no. 100182.

Shen, T., Wang, F., Chen, K., Wang, K., and Li, B., 2019. Efficient leveled (multi) identity-based fully homomorphic encryption schemes. IEEE Access, 7, pp. 79299–79310. Available at: https://doi.org/10.1109/ACCESS.2019.2922685 [Accessed 20 Nov. 2024].

Sultan, Nora. “IMAGE COMPRESSION BY USING WALSH AND FRAMELET TRANSFORM ”. Kufa Journal of Engineering, vol. 10, no. 2, June 2021, pp. 27-41, https://doi.org/10.30572/2018/KJE/100203.

Tan, W., Yan, B., Li, K. and Tian, Q., 2016. Image retargeting for preserving robust local feature: Application to mobile visual search. IEEE Transactions on Multimedia, 18(1), pp. 128–137. Available at: https://doi.org/10.1109/TMM.2015.2500727 [Accessed 20 Nov. 2024].

Tsai, S., Chen, H., Chen, D., Vedantham, R., Grzeszczuk, R., and Girod, B., 2011. Mobile visual search using image and text features. 2011 Conference Record of the Forty-Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, pp. 845–849. Available at: https://doi.org/10.1109/ACSSC.2011.6190127 [Accessed 20 Nov. 2024].

Xu, D., Lu, Y., and Li, L., 2021. Embedding blockchain technology into IoT for security: a survey. IEEE Internet of Things Journal, 8(13), pp. 10452–10473. Available at: https://doi.org/10.1109/JIOT.2021.3060508 [Accessed 20 Nov. 2024].

Yang, N., Tang, C., and He, D., 2024. A lightweight certificateless multi-user matchmaking encryption for mobile devices: Enhancing security and performance. IEEE Transactions on Information Forensics and Security, 19, pp. 251–264. Available at: https://doi.org/10.1109/TIFS.2023.3321961 [Accessed 20 Nov. 2024].